UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1

CONFIRMATION NO. 7326

POA ACCEPTANCE LETTER

109422
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 408
Austin, TX 78705

OC000000116298641

Date Mailed: 04/21/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sibrahim/

Trend Micro, Inc.
EX1006-1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1

CONFIRMATION NO. 7326

POWER OF ATTORNEY NOTICE

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

OC000000116298609

Date Mailed: 04/21/2020

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sibrahim/

Trend Micro, Inc.
EX1006-2

Power of Attorney to Transact Business with the United States Patent and Trademark Office

I hereby revoke all previous Powers of Attorney given in the application(s) identified in the attached Transmittal for Power of Attorney to One or More Registered Practitioners ("Transmittal Form").

I hereby appoint practitioners associated with the following Customer Number associated with Sprinkle IP Law Group, PC :

109422

as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **Webroot Inc.** (the "assignee's patents/patent applications") in which they shall appear, any and all assignee's patents/patent applications associated with the above-referenced customer number, and any and all patents and patent applications referenced in the attached Transmittal Form.

Please recognize or change the correspondence address for the patents and patent applications referenced in the attached Transmittal Form to the address associated with the above-referenced customer number.

The undersigned is:

- ☐ Inventor or Joint Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
  *the undersigned has authority to act on behalf of the Assignee or Person to Whom the Inventor is Under an Obligation to Assign.
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is currently being filed in this document)

The Transmittal Form may be completed and executed by one of the practitioners associated with the above-referenced customer number.

SIGNATURE OF APPLICANT

Signature:		**Date:**	January 29, 2020
Name:	**Gordon A. Davies**		
Title:	Director		
Company:	**Webroot Inc.**		

I am authorized to act on behalf of the assignee.

Trend Micro, Inc.
EX1006-3

Electronic Acknowledgement Receipt

EFS ID:	39155554
Application Number:	14606604
International Application Number:	
Confirmation Number:	7326
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Customer Number:	23552
Filer:	John L. Adair/keunah cheun
Filer Authorized By:	John L. Adair
Attorney Docket Number:	04584.0117USU1
Receipt Date:	14-APR-2020
Filing Date:	27-JAN-2015
Time Stamp:	15:33:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	WEBROOT_POA_012820.pdf	42303 460c019d47e52952aad549f0d335131a49b6cfef	no	1

Warnings:

Information:	
Total Files Size (in bytes):	42303

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	05/07/2019	10284591	04584.0117USU1	7326

23552 7590 04/17/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 160 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Marco Giuliani, Bastia Umbra (PG), ITALY;
WEBROOT INC., Broomfield, CO;
Marco Bizzarri, Sassoferrato (AN), ITALY;
Benedetto Voltattorni, San Benedetto del Tronto (AP), ITALY;
Johannes Mayr, Linz, AUSTRIA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT
Conf. No. 7326

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Giuliani et al.	Examiner:	GYORFI, THOMAS A.
Serial No.:	14/606,604	Group Art Unit:	2435
Filed:	January 27, 2015	Docket No.:	04584.0117USU1
Title:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS		

COMMENTS ON EXAMINER STATEMENT

Mail Stop – ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Washington, D.C. 20231

Dear Commissioner:

Applicant acknowledges the allowance of claims 1, 3-10, and 12-20 in the subject application by the Examiner with appreciation. Although the Examiner did not issue a Statement of Reasons for Allowance, Applicant agrees with statements made by the Examiner during the prosecution of the present application to the extent that the claims of the present invention are patentable over the references in the record. However, Applicant does not necessarily acquiesce or agree in any manner as to comments made by the Examiner regarding what the prior art does or does not teach. In addition, Applicant respectfully traverses statements made by the Examiner to the extent that any comment is intended or has the effect of limiting a claim scope, explicitly or implicitly, by not reciting verbatim the respective claim language, or is intended or has the effect of limiting a claim scope by stating or implying that all the reasons for patentability are in any way fully enumerated.

Further reasons for allowance are described and set forth in the Applicant's Specification. As the Examiner's statements are not exhaustive, such statements do not establish an estoppel against Applicant seeking and obtaining allowance of additional, broader claims in a continuation application, which Applicant reserves the right to file.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

Respectfully submitted,

Date: March 20, 2019

/Andrew T. Pouzeshi/

Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 12/20/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1	7326

TITLE OF INVENTION: DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	03/20/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
GYORFI, THOMAS A	2435	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Merchant & Gould P.C.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: WEBROOT INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Broomfield, CO

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 132725

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Andrew T. Pouzeshi/ Date March 20, 2019

Typed or printed name Andrew T. Pouzeshi/ Registration No. 67672

Trend Micro, Inc.
EX1006-9

Electronic Patent Application Fee Transmittal

Application Number:	14606604
Filing Date:	27-Jan-2015
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0117USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1000**

Electronic Acknowledgement Receipt

EFS ID:	35484575
Application Number:	14606604
International Application Number:	
Confirmation Number:	7326
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0117USU1
Receipt Date:	20-MAR-2019
Filing Date:	27-JAN-2015
Time Stamp:	18:33:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1000
RAM confirmation Number	032119INTEFSW18345800
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Post Allowance Communication - Incoming	2019-03-20-Comments-04584-0117USU1.PDF	71188 301fb4a22ea0721a0fc8419628fc1a1ae9392742	no	2
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	2019-03-20-IssueFee-04584-0117USU1.PDF	125005 bbf552fe6fa9007726aa478c491189ad5e366508	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30474 9effd21cee11a7348cd65c5411c0ef064dfc5168	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	226667		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23552 7590 12/20/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2435	

DATE MAILED: 12/20/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1	7326

TITLE OF INVENTION: DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	03/20/2019

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Trend Micro, Inc.
EX1006-14

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 12/20/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1	7326

TITLE OF INVENTION: DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	03/20/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
GYORFI, THOMAS A	2435	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Trend Micro, Inc.
EX1006-15

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1	7326

23552 7590 12/20/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2435	

DATE MAILED: 12/20/2018

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Trend Micro, Inc.
EX1006-16

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/606,604	Applicant(s) Giuliani et al.	
	Examiner THOMAS A GYORFI	Art Unit 2435	AIA Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to the amendment filed 10/1/18.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1,3-10 and 12-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/THOMAS A GYORFI/ Examiner, Art Unit 2435	/JOSEPH P HIRL/ Supervisory Patent Examiner, Art Unit 2435

Trend Micro, Inc.
EX1006-18

Notice of Pre-AIA or AIA Status

1. Claims 1, 3-10, and 12-20 remain for examination. The amendment filed 10/1/18 amended claims 1, 4, 8, 10, 13, 17, & 19; and cancelled claims 2 & 11. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

2. Applicant's arguments, see pages 9-11 of the amendment filed 10/1/18, with respect to Salaam and Yeap have been fully considered and are persuasive. The rejection of claims 1-20 has been withdrawn.

Allowable Subject Matter

3. Claims 1, 3-10, and 12-20 are allowed.

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THOMAS A GYORFI whose telephone number is (571)272-3849. The examiner can normally be reached on 10:00am - 6:30pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on 571-272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

THOMAS A. GYORFI
Examiner
Art Unit 2435

/THOMAS A GYORFI/
Examiner, Art Unit 2435
12/12/18

/JOSEPH P HIRL/
Supervisory Patent Examiner, Art Unit 2435

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/606,604	Giuliani et al.
	Examiner	**Art Unit**
	THOMAS A GYORFI	2435

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L 63/1408, 1441	12/9/16	TAG
G06F 21/52, 554	12/9/16	TAG
H04L 63/1408, 1441	8/24/17	TAG
G06F 21/52, 554	8/24/17	TAG
H04L 63/1408, 1441	3/19/18	TAG
G06F 21/52, 554	3/19/18	TAG
H04L 63/1408, 1441	12/12/2018	TAG
G06F 21/52, 554	12/12/2018	TAG

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
EAST search	12/9/16	TAG
NPL search (Google)	12/9/16	TAG
EAST search (updated)	8/24/17	TAG
EAST search (updated)	3/19/18	TAG
EAST search (updated)	12/12/2018	TAG

/THOMAS A GYORFI/ Examiner, Art Unit 2435	

Trend Micro Inc.
EX1006-21

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/606,604	Giuliani et al.
	Examiner	**Art Unit**
	THOMAS A GYORFI	2435

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
H04L	63/1408, 1441	12/12/2018	TAG
G06F	21/52, 554	12/12/2018	TAG

/THOMAS A GYORFI/ Examiner, Art Unit 2435	

Trend Micro Inc.
EX1006-22

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/606,604	Giuliani et al.
	Examiner	**Art Unit**
	THOMAS A GYORFI	2435

CPC						
Symbol					**Type**	**Version**
H04L	/	63	/	1441	F	2013-01-01
G06F	/	21	/	554	I	2013-01-01
H04L	/	63	/	1408	I	2013-01-01
G06F	/	21	/	52	I	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

/THOMAS A GYORFI/ Examiner, Art Unit 2435 (Assistant Examiner)	12 December 2018 (Date)	**Total Claims Allowed:** 18	
/JOSEPH P HIRL/ SPE, Art Unit 2435 (Primary Examiner)	14 December 2018 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

U.S. Patent and Trademark Office

Part of Paper No.: 20181212

Trend Micro, Inc.
EX1006-23

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/606,604	Giuliani et al.
	Examiner	**Art Unit**
	THOMAS A GYORFI	2435

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04L	/	29	/	06

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

/THOMAS A GYORFI/ Examiner, Art Unit 2435 (Assistant Examiner)	12 December 2018 (Date)	**Total Claims Allowed:** 18	
/JOSEPH P HIRL/ SPE, Art Unit 2435 (Primary Examiner)	14 December 2018 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

U.S. Patent and Trademark Office

Part of Paper No.: 20181212

Trend Micro, Inc.
EX1006-24

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/606,604	Giuliani et al.
	Examiner	**Art Unit**
	THOMAS A GYORFI	2435

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	9	10	17	19										
	2		11	18	20										
2	3	10	12												
3	4	11	13												
4	5	12	14												
5	6	13	15												
6	7	14	16												
7	8	15	17												
8	9	16	18												

/THOMAS A GYORFI/ Examiner, Art Unit 2435 (Assistant Examiner)	12 December 2018 (Date)	**Total Claims Allowed:** 18	
/JOSEPH P HIRL/ SPE, Art Unit 2435 (Primary Examiner)	14 December 2018 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

U.S. Patent and Trademark Office

Part of Paper No.: 20181212

Trend Micro, Inc.
EX1006-25

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/606,604	Giuliani et al.
	Examiner	**Art Unit**
	THOMAS A GYORFI	2435

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/09/2016	08/24/2017	03/19/2018	12/12/2018					
1	1	✓	✓	✓	=					
	2	✓	✓	✓	-					
2	3	✓	✓	✓	=					
3	4	✓	✓	✓	=					
4	5	✓	✓	✓	=					
5	6	✓	✓	✓	=					
6	7	✓	✓	✓	=					
7	8	✓	✓	✓	=					
8	9	✓	✓	✓	=					
9	10	✓	✓	✓	=					
	11	✓	✓	✓	-					
10	12	✓	✓	✓	=					
11	13	✓	✓	✓	=					
12	14	✓	✓	✓	=					
13	15	✓	✓	✓	=					
14	16	✓	✓	✓	=					
15	17	✓	✓	✓	=					
16	18	✓	✓	✓	=					
17	19	✓	✓	✓	=					
18	20	✓	✓	✓	=					

Trend Micro, Inc.
EX1006-26

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	15129	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/12/12 19:23
L2	15102	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/12/12 19:23
L3	6386	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/12/12 19:23
L4	10602	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/12/12 19:23
L5	27193	(L1 L2 L3 L4) and @ad< "20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/12/12 19:23
L6	1	("20120255018").PN.	US-PGPUB; USPAT	OR	OFF	2018/12/12 19:31
S1	1	("20150215335").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:21
S2	0	("2014033132220150020202").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:22
S3	2	(("20140331322") or ("20150020202")).PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:22
S4	10085	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:28
S5	10411	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S6	4638	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29

S7	7140	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S8	24673	(S4 S5 S6 S7) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S9	5	("20050108562" | "20110145924" | "20120255013" | "20120255018" | "8510596").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:31
S10	10085	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S11	10411	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S12	4638	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S13	7140	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S14	24673	(S10 S11 S12 S13) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S15	17	S14 and stack adj walk$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S16	55	S14 and base adj pointer	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S17	498	S14 and virtual adj memory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S18	43	S17 and (S15 S16)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S19	70	(S15 S16)	US-PGPUB; USPAT; FPRS;	OR	OFF	2016/12/09 17:53

			EPO; JPO; DERWENT; IBM_TDB			
S20	2	(S15 and S16)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S21	1	S18 and S20	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S22	21	ntallocatevirtualmemory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S23	19	ntprotectvirtualmemory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S24	27	ntcreateprocess	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S25	5	ntcreateprocessex	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S26	0	ntcreateuseriprocess	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:58
S27	14	ldrloaddll	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:58
S28	2	S22 S23 S24 S25 S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 17:58
S29	2	(S22 S23 S24 S25) or (S22 S23 S25 S27) or (S22 S24 S25 S27) or (S23 S24 S25 S27)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 17:59
S30	2	(S22 S23 S24) or (S22 S23 S25) or (S22 S23 S27) or (S23 S24 S25) or (S23 S24 S27) or (S24 S25 S27)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 18:00
S31	5	("20050108562" | "20110145924" | "20120255013" | "20120255018" |	US-PGPUB; USPAT	OR	OFF	2016/12/09 18:12

		"8510596").PN.				
S32	2	S31 and (S22 S23 S24 S25 S27)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 18:12
S33	1	("20120255018").PN.	US-PGPUB; USPAT	OR	OFF	2017/08/24 13:00
S34	11779	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S35	11993	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S36	5257	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S37	8224	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S38	26121	(S34 S35 S36 S37) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S39	674	S38 and (hook shim)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:03
S40	308	S39 and ((hook shim) same (process memory space))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:03
S41	94	S39 and ((hook shim) same (monitor$3 with (process memory space)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:04
S42	12841	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
S43	12957	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
S44	5616	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT;	OR	OFF	2018/03/19 09:22

			IBM_TDB			
S45	8877	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
S46	26580	(S42 S43 S44 S45) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
S47	3682	giuliani.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:51
S48	719	bizzarri.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:51
S49	99	voltattorni.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52
S50	7205	mayr.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52
S51	506	(S47 S48 S49 S50) and (marco benedetto johannes).in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52
S52	1	S51 and S46	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L8	96200	(hook shim).clm.	USPAT	OR	OFF	2018/12/12 19:44
L9	12303	((process memory) near3 space).clm.	USPAT	OR	OFF	2018/12/12 19:44
L10	85	l8 and l9	USPAT	OR	OFF	2018/12/12 19:44
L11	19720	(plurality near3 function).clm.	USPAT	OR	OFF	2018/12/12 19:45
L12	9	(stack adj walk).clm.	USPAT	OR	OFF	2018/12/12 19:46
L13	165	(stack adj entr$3).clm.	USPAT	OR	OFF	2018/12/12 19:46
L14	201	l11 and (l8 l9 l12 l13)	USPAT	OR	OFF	2018/12/12 19:46

12/12/2018 7:47:00 PM
C:\Users\tgyorfi\Documents\EAST\Workspaces\14606604.wsp

PATENT
Conf. No. 7326

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Giuliani et al.	Examiner:	GYORFI, THOMAS A.
Serial No.:	14/606,604	Group Art Unit:	2435
Filed:	January 27, 2015	Docket No.:	04584.0117USU1
Title:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS		

AMENDMENT & RESPONSE TO NON-FINAL OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Non-Final Office Action mailed March 30, 2018, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on page 2 of this paper.

Remarks/Arguments begin on page 8 of this paper.

Trend Micro, Inc.
EX1006-33

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer-implemented method comprising:

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

invoking one of the plurality of functions as a result of receiving a call from an application programming instance;

executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing before an address of an originating caller function is reached, ~~at least one~~ a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when~~, during~~ the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

2. (Canceled)

3. (Original) The method according to claim 1, further comprising:

identifying an address associated with the invoked function; and

when the address of the invoked function address is found in a cache, preventing execution of a payload for the invoked function.

4. (Currently Amended) The method according to claim 1, wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to ~~an~~the originating address of the invoked function.

5. (Original) The method according to claim 1, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

6. (Original) The method according to claim 1, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

7. (Original) The method according to claim 1, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

8. (Currently Amended) The method according to claim 6, wherein performing the ~~one or more~~ memory ~~checks~~check comprises evaluating state information associated with a cache entry for the hooked function.

9. (Original) The method according to claim 8, wherein when an address of the invoked function is found in a cache, preventing execution of a payload for the invoked function.

10. (Currently Amended) A system comprising:

at least one memory; and

at least one processor connected with the memory configured to perform operation of:

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

invoking one of the plurality of functions as a result of receiving a call from an application programming instance;

executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing before an address of an originating caller function is reached, ~~one or more memory checks~~a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when~~, during~~ the performing ~~of the one or more memory checks detects~~ of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, the method further comprising preventing execution of a payload for the invoked function.

11. (Canceled)

12. (Original) The system according to claim 10, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is

found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

13. (Currently Amended) The system according to claim 10, wherein the executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to ~~an~~the originating address of the invoked function.

14. (Original) The system according to claim 10, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

15. (Original) The system according to claim 10, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, and wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

16. (Original) The system according to claim 10, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

17. (Currently Amended) The system according to claim 15, wherein performing of the memory ~~checks~~ check comprises evaluating state information associated with a cache entry for the hooked function.

18. (Original) The system according to claim 17, wherein when an address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

19. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

invoking one of the plurality of functions as a result of receiving a call from an application programming instance;

executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing before an address of an originating caller function is reached, ~~at least one~~a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack,

a return address is detected as being inside a virtual memory area, and

a low level user mode function is attempted to be executed in a cache, wherein the cache is evaluated for an address of the invoked function, and

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function.

20. (Original) The computer-readable storage device according to claim 19, wherein performing of the memory check to determine if code execution is attempted from non-executable memory, the base pointer is identified as being invalid, an invalid stack return address

Trend Micro, Inc.
EX1006-38

is identified, execution of a return-oriented programming technique is attempted, the base pointer is detected as being outside a current thread stack, and the return address is detected as being inside a virtual memory area, occurs before an address of the invoked function is reached, and

wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing.

Trend Micro, Inc.
EX1006-39

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the non-final Office Action dated March 30, 2018, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claims 1-6, 8-15, and 17-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam (U.S. Publ. No. 2012/0255018; hereinafter "Sallam") in view of Yeap (U.S. Publ. No. 2007/0016914; hereinafter "Yeap"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam in view of Yeap as applied to claims 1 and 10, and further in view of Kolsek et al. (U.S. Publ. No. 2005/0108562; hereinafter "Kolsek").

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 4, 8, 10, 13, 17, and 19 have been amended, claims 2 and 11 have been canceled. Therefore, claims 1, 3-10, and 12-20 remain present for examination.

Applicants submit that claim amendments are supported throughout the specification, and in the claims as originally filed, and do not introduce new matter. For instance, the amendments are supported by at least the following sections of the Specification: ¶¶ [0022]-[0026].

Claim Rejections Under § 103:

Claims 1-6, 8-15, and 17-20

Claims 1-6, 8-15, and 17-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam in view of Yeap. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

In nonexclusive, non-limiting examples, the present disclosure is generally directed to systems and methods for monitoring a memory space of a process. In some aspects, monitoring the memory space includes execution of a stack walk, which is initiated upon invocation of a function call from an application program or application program interface. More specifically, a stack walk processing is executed which walks up a call stack for the process (function) until an address of the first function of a called function is reached. *See e.g., Applicant's specification-as-published,* ¶ [0022]. During the stack walk processing, one or more stack entries may be found. *See e.g., Id.,* at ¶ [0023]. The stack walk processing performs a memory check or checks on a frame of call stack pertaining to the called process (including one or more functions) attempting to detect and identify suspicious behavior that may pertain to a software exploit. *See e.g., Id.,* at ¶ [0026]. Examples of memory checks performed are provided in a later description of FIG. 2. *See e.g., Id.* Unlike other exploit prevention technologies that try to prevent that an exploit starts its own shellcode, the anti-exploit examples implemented by the anti-exploit component prevent that the shellcode performs an ultimate execution of a malicious payload, whether the malicious payload is loading another module or executing another process. *See e.g., Id.*

Turning specifically to the claims, Claim 1 recites, in part,

> monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;
>
> invoking one of the plurality of functions as a result of receiving a call from an application programming instance;
>
> executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and
>
> performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:

See e.g., Claim 1.

In contrast, the primary reference of Sallam generally relates to a security agent configured to execute on the electronic device at a level below all of the operating systems of the electronic device accessing the memory or a storage of the electronic device. As part of the

disclosure, Sallam discusses instances where "VMM security agent 217 may be configured to determine contextual information, such as what entity of operating system 212 has attempted to access a resource of electronic device 204, or to what entity of operating system 212 a resource may belong." *See e.g., Sallam,* at ¶ [0060]. Sallam further disclose that the "SVMM security agent 217 may be configured to, directly or indirectly, access a call stack of operating system 212 and/or an execution stack of processor 208 to determine the order of calls made by different processes or applications of operating system 212 accessing the stack." *See e.g., Id.* " *See e.g., Sallam,* at ¶ [0060]. Sallam's disclosure of accessing the stack, however, is distinguishable from the current application because the stack walk processing of the present disclosure occurs as a result of a call from a programming application (e.g., an application that may be malicious). That is, Sallam does not invoke a monitored function as a result of receiving a call from an application programming instance. Further, while Sallam discloses "walking through the Execution Base Pointer through the stack" which may identify "previous function calls" to provide "context for the operation at hand" (*See e.g., Id.*), there is no disclosure within Sallam directed to performing the claimed memory check "for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior" "during the executing of the stack walk processing before an address of an originating caller function is reached." That is, there is no disclosure within Sallam indicating that the pointer and virtual memory conditions in paragraphs [0239]-[0242] to which the Examiner refers are performed during the stack walk processing as claimed. The addition of Yeap fails to teach that which Sallam lacks.

Rather, Yeap is generally directed to a scheme whereby an API interception application 106 that "can intercept all user mode call threads directed to the kernel mode API 114." *See e.g., Yeap,* at ¶ [0024]. As evident in Fig. 1, the API interception application of Yeap is prior to the kernel mode. It is thus, the intention of Yeap to prevent calls that require interaction with the kernel to be intercepted and analyzed for malicious software. Yeap teaches injecting a hook into machine instruction for one or more particular types of calls and then redirecting the call to the API interception application 106. *See e.g., Id.* at ¶ [0026]. While Yeap further teaches that an "analysis engine 204 can examine the call to identify the previous operations performed from the point at which the call was first initiated" and that "the analysis engine 204 can perform a stack backtracking to identify previous steps in the call history, (*See e.g., Id.* at ¶ [0037]) there is no

indication that Yeap teaches performing the claimed memory check "for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior" "during the executing of the stack walk processing before an address of an originating caller function is reached." This simply is not provided by Yeap. As Sallam and Yeap disclose, teach, or suggest at least the combination of features claimed, Applicant respectfully submits that claim 1 is allowable over Sallam in view of Yeap.

For at least similar reasons, independent claim 10 is also allowable. Claim 10 recites, *inter alia*, "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior." Thus, claim 10 is allowable for at least similar reasons as discussed with respect to independent claim 1.

Independent claim 19 is also allowable for at least similar reasons. Claim 19 recites, *inter alia*, "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior. Thus, claim 19 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1, 10, and 19 were allowable over the cited Sallam. All other claims, i.e., claims 3-6, 8-10, 12-15, and 17-20, depend from one of allowable claims 1, 10, or 19 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 1, 3-6, 8-10, 12-15, and 17-20.

<u>Claims 7 and 16</u>

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam in view of Yeap as applied to claims 1 and 10, and further in view of Kolsek in view of

Trend Micro, Inc.
EX1006-43

Khazan. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

For at least the reasons discussed above, claim 1 is allowable over Sallam in view of Yeap. Applicants respectfully submit that Kolsek fails to compensate for the deficiencies of Sallam's and/or Yeap deficiencies. Kolsek generally relates to observing the calls of system and application functions, and the arguments of such calls, which play a key role in loading executable files, and detects that a computer program or operating system either has tried, is trying or will try to load or execute an executable file from the current working directory. Kolsek, however, fails to teach or suggest at least "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior" as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Sallam, Yeap, and Kolsek.

Khazan fails as well. Khazan generally relates to automatic detection of malicious code by verifying that an application executes in accordance with a model defined using calls to a predetermined set of targets, such as external routines. A model is constructed using a static analysis of a binary form of the application, and is comprised of a list of calls to targets, their invocation and target locations, and possibly other call-related information. Khazan, however, fails to teach or suggest at least "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing,

during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior" as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Sallam, Yeap, Kolsek, and Khazan.

For at least similar reasons, independent claim 10 is also allowable. Claim 10 recites, *inter alia*, "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior." Thus, claim 10 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 10 are allowable over the cited references. Claims 7 and 16 depend from one of allowable claims 1 or 10 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 7 and 16.

CONCLUSION

This Amendment fully responds to the Office Action mailed on March 30, 2018. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicants believe the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Petition for Extension of Time. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: October 1, 2018

/Brent R Lindon/

Brent R. Lindon, Reg. No. 67,424
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1182

23552
PATENT TRADEMARK OFFICE

Trend Micro, Inc.
EX1006-46

PTO/AIA/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0117USU1

Application Number: 14/606,604

Filed: January 27, 2015

For: DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

Art Unit: 2435

Examiner: GYORFI, THOMAS A.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1400
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132725.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 67424.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Brent R Lindon/
Signature

2018-10-01
Date

Brent R. Lindon
Typed or printed name

(303) 357-1182
Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14606604
Filing Date:	27-Jan-2015
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Filer:	Brent Robert Lindon/Brittany Andersen
Attorney Docket Number:	04584.0117USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
			Total in USD ($)	**1400**

Electronic Acknowledgement Receipt

EFS ID:	33883979
Application Number:	14606604
International Application Number:	
Confirmation Number:	7326
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Customer Number:	23552
Filer:	Brent Robert Lindon/Brittany Andersen
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	04584.0117USU1
Receipt Date:	01-OCT-2018
Filing Date:	27-JAN-2015
Time Stamp:	16:45:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1400
RAM confirmation Number	100218INTEFSW16462400
Deposit Account	132725
Authorized User	Brittany Andersen

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2018-10-01_AMD_04584-0117USU1.pdf	167414 397c0f96148654028293d1f252f487589c5feea2	yes	14
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	7	
	Applicant Arguments/Remarks Made in an Amendment		8	14	
Warnings:					
Information:					
2	Extension of Time	2018-10-01_EOT_04584-0117USU1.pdf	140922 7a019fb90ee41791f2b5cebcb5d7a1cb39bb3a26	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31126 d4bc9db322a28cda6148cf27e3f0f523a94eb734	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	339462		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY.DOCKET NO./TITLE	REQUEST ID
14/606,604	01/27/2015	WEBROOT INC.	04584.0117USU1	72771

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 10/01/2018 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

X Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/Andrew T. Pouzeshi/
Name:	Andrew T. Pouzeshi
Registration Number:	67672

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
14/606,604	01/27/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	x $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	x $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT

10/01/2018	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0	x $100 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	x $460 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
CURTIS NELLOMS JR

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1	7326

23552 7590 03/30/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
03/30/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Trend Micro, Inc.
EX1006-56

Office Action Summary	Application No. 14/606,604	Applicant(s) GIULIANI ET AL.	
	Examiner Thomas Gyorfi	Art Unit 2435	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 2/28/18.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) 1-20 is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Trend Micro, Inc.
EX1006-57

DETAILED ACTION

1. Claims 1-20 remain for examination. The amendment filed 2/28/18 amended claims 1, 10, and 19. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/28/18 has been entered.

Response to Arguments

3. Applicant's arguments filed 2/28/18 have been fully considered but they are not persuasive. Regarding claim 1 and the Yeap reference, Applicant argues:

> In contrast to the present technology, Yeap does not allow software to cause system resources to be manipulated (e.g., enter the kernel mode) as a result of a system call from an API, prior to performing a security check. Rather, Yeap provides a scheme whereby an API interception application 106 that "can intercept all user mode call threads directed to the kernel mode API 114." Yeap at [0024]. As evident in Fig. 1, the API interception application of Yeap is prior to the kernel mode. It is thus, the intention of Yeap to prevent calls that require interaction with the kernel to be intercepted and analyzed for malicious software. Indeed, Yeap explicitly states as much, noting: "[I]n one implementation, the API interception application is part of a security system. . . . The security system can examine intercepted calls to prevent the malicious software from being transported into the kernel layer using the call command." Yeap at [0026] (emphasis added). As such, Yeap would never allow the execution of a stack walk, which is a system process, in response to a function call by an application, as the claims require.

Examiner disagrees, first by noting that the analysis engine which performs the actual step of determining if it is safe to execute the requested kernel function call can inter alia perform a "stack backtracking" to examine the call history; and if any suspect steps in the call thread are identified, the kernel mode call can be denied (Yeap, at paragraph 0037). Although Yeap does not go into more detail as to how this analysis engine component can identify a suspect step, nevertheless this process appears to be substantially similar to the stack walking process disclosed by Salaam, which as previously cited does explicitly recite the claimed conditions that would indicate that a function call should be denied execution. Second, although the calls being intercepted by Yeap are made in user mode memory space, the kernel validation layer including the aforementioned analysis engine are specifically included as part of the protected kernel mode space (see Figures 1 & 2); thus the analysis engine – contrary to Applicant's assertion – can and does allow the execution of a stack walk in response to a function call by an application, as the claims require.

Further regarding Yeap, Applicant additionally argues:

> The Office appears to interpret Yeap paragraphs [0024]-[0028] to interpret that a security evaluation is passed at the kernel level. Office Action at 4 (noting: "A User Mode API Interception Application ... inserts one or more hooks into said user application to monitor their use of one or more system call functions, which relays the call information to a kernel mode component that performs the security evaluation: paragraphs 0024-0028, and Figure 1."(emphasis added)). Applicants respectfully disagree with the Office's interpretation of Yeap. In particular, Fig. 1 of Yeap explicitly provides that the API interception application 106 is in the user mode:
>
> [...]
>
> As the API 106 performs the security check and creates an interrupt 107 prior to the call entering the kernel mode, Applicants submit that no system actions are performed under Yeap as a result of receiving a call.
>
> In short, whereas Yeap interrupts a system call from an API prior to entering the kernel mode, aspects of the technology execute a stack walk upon an invocation of a system

> call from an API. To clarify this distinction, Applicants have amended claim 1 to include "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space." Thus, claim 1 is allowable over Saliam in view of Yeap.

Examiner disagrees, again pointing to paragraph 0037 of Yeap wherein the analysis engine – which is itself a system call in kernel space invoked by the hook function in user space – is a system action that performs a stack walking function to determine if the actual kernel mode call should be permitted. However, it should be noted that, although the claims recite that the monitored functions may exist within a protected memory space, technically there is no requirement that the function(s) that perform the stack walk etc. themselves must necessarily be system calls; thus even if Yeap did not disclose this functionality, it would not have been required by the claims.

Examiner also wishes to note that Applicant appears to be drawing a distinction between the method of operation of Yeap in particular versus the instant invention, by arguing that Yeap's hooked functions are somehow substantively different from the means by which the instant invention performs the equivalent protection feature. As per the preferred embodiment of paragraphs 0019-0022 of the instant specification as originally filed, the instant invention creates a plurality of hooked functions (one for each system call to be protected, including the specifically named Windows function calls specifically recited in dependent claims 7 & 16) such that, when an application attempts to invoke the system call, instead (and unbeknownst to said application) invoked the hooked function instead, which includes additional code of the Applicant's design to perform a stack walk to determine if the actual system call is safe to execute, and deny the execution of the system call if it is determined to be unsafe. Applicant appears to

acknowledge that Yeap operates in this fashion, yet insists without support that this is patentably distinct from the instant invention. The Examiner does not see any patentable distinction, and maintains that Yeap, which invokes one of its plurality of [hooked] functions as a result of receiving a call from an application programming instance, reads on the claimed subject matter.

Applicant's arguments against the Salaam reference presented earlier (pages 7-8 of the amendment of 2/28/18) are moot in view of the fact that the rejection was based on the combination of Salaam with Yeap, and as discussed supra Yeap discloses the limitation(s) alleged to not be disclosed by Salaam; thus the combination continues to disclose or suggest the claimed subject matter.

Applicant's arguments traversing independent claims 10 & 19 is substantially similar to those traversing claim 1, and are rebutted as discussed supra. Dependent claims 2-9, 11-18, and 20 follow from independent claims 1, 10, & 19 and are similarly rejected. Additionally, Applicant's arguments traversing the rejection of claim 7 and 16 in view of Salaam, Yeap, and Kolsek and Khazan are rebutted as substantially similar above, as Yeap discloses the limitations that Applicant alleges are not taught by Kolsek or Khazan.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claim 1-6, 8-15, and 17-20 are rejected under 35 U.S.C. 103 as being unpatentable over Salaam (U.S. Patent Publication 2012/0255018) in view of Yeap (U.S. Patent Publication 2007/0016914).

Regarding claims 1, 10, and 19:

Salaam discloses a computer-implemented method, system, and computer storage device comprising: monitoring a memory space of a process for execution of at least one of a plurality of functions (paragraph 0077); executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space (paragraph 0060); and performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior (Ibid), wherein an alert of suspicious behavior is triggered when, during the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating (pointer and virtual memory conditions at paragraphs 0239-0242). Per claim 10, Salaam further discloses a memory and processor (paragraphs 0045-0046).

Salaam appears to be silent regarding wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space. However, Yeap discloses a related invention for monitoring the memory space of an process for execution comprising this limitation (a User Mode API Interception Application, running in the same user mode memory space as the user applications, inserts one or more hooks into said user applications to monitor their use of one or more system call functions; when a user mode API tries to invoke one of the plurality of hooked functions, the function relays the call information to a kernel mode component that performs the security evaluation: paragraphs 0024-0028, and Figure 1). It would have been obvious to install hooks into the processes monitored by Salaam, as this approach can be used to detect if malware has hijacked a process and thwart its execution (Yeap, Ibid, particularly paragraphs 0026-0028).

Regarding claims 2 and 11:

The combination further discloses wherein performing the memory check occur before an address of an originating caller function is reached (Salaam: paragraph 224).

Regarding claims 3 and 12:

The combination further discloses further comprising: identifying an address associated with the invoked function (Salaam: paragraph 0067); and when the address of the invoked function address is found in a cache, preventing execution of a payload for the invoked function (Salaam: paragraphs 0138 & 0211).

Regarding claims 4 and 13:

The combination further discloses wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function (Salaam: paragraph 0060).

Regarding claims 5 and 14:

The combination further discloses wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function (Salaam: paragraphs 0039 & 0042).

Regarding claims 6 and 15:

The combination further discloses wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function (Salaam: paragraphs 0039, 0049, & 0090), wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function (Salaam: Ibid, and paragraph 0060).

Regarding claims 8 and 17:

The combination further discloses wherein performing the one or more memory checks comprises evaluating state information associated with a cache entry for the hooked function (Salaam: paragraphs 0090, 0193, 0207, 0214, & 0269).

Regarding claims 9 and 18:

The combination further discloses wherein when an address of the invoked function is found in a cache, preventing execution of a payload for the invoked function (Salaam: paragraphs 0138 & 0211).

Regarding claim 20:

The combination further discloses wherein performing of the memory check to determine if code execution is attempted from non-executable memory, the base pointer is identified as being invalid (Salaam: paragraph 0276), an invalid stack return address is identified (Salaam: paragraphs 0049 & 0060), execution of a return-oriented programming technique is attempted (Salaam: paragraph 0117), the base pointer is detected as being outside a current thread stack (Salaam: paragraphs 0049 & 0060), and the return address is detected as being inside a virtual memory area (Salaam: paragraphs 0239-0240), occurs before an address of the invoked function is reached (Salaam: paragraph 0224), and wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing (Salaam: paragraphs 0039, 0207, and 0224).

6. Claims 7 & 16 are rejected under 35 U.S.C. 103 as being unpatentable over Salaam in view of Yeap as applied to claims 1 & 10 above, and further in view of Kolsek (U.S. Patent Publication 2011/0145924) in view of Khazan (U.S. Patent Publication 2005/0108562).

Regarding claims 7 and 16:

Although Salaam discloses an open-ended list of functions that can be monitored by his invention, explicitly including wherein the plurality of functions comprises the NtAllocateVirtualMemory and NtProtectVirtualMemory functions (paragraph 0283), nevertheless Salaam and Yeap are silent regarding the NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function. However, Kolsek discloses a related invention for preventing the execution of malware by *inter alia* monitoring and intercepting function calls including NTCreateProcess, NtCreateUserIProcess, and LdrLoadDLL (paragraphs 0049-0065). It would have been obvious to modify Salaam to also monitor these particular functions, as these functions were known to present a vulnerability that would allow malicious hackers to plant malware in a way that was not previously detectable by the prior art (Kolsek, paragraphs 0014-0020 & 0038).

Neither Salaam, Yeap, nor Kolsek names the NTCreateProcessEx function. However, Khazan discloses a similar invention for detecting malware wherein an analyzer is triggered upon invocation of NTCreateProcessEx (Khazan, paragraph 0076). It would have been obvious for Salaam to also monitor NTCreateProcessEx, as

this technique allows for detection of both known and unknown threats (Khazan, paragraphs 0009-0010).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: U.S. Patent 7313,821 (Steiner).

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 10:00am - 6:30pm Monday - Friday.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on (571) 272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thomas Gyorfi/
Examiner, Art Unit 2435
3/19/18

Notice of References Cited	Application/Control No. 14/606,604	Applicant(s)/Patent Under Reexamination GIULIANI ET AL.	
	Examiner Thomas Gyorfi	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-7,313,821 B1	12-2007	Steiner; Thomas C. H.	G06F21/554	714/E11.207
	B	US-				
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1006-69

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14606604	GIULIANI ET AL.
	Examiner	**Art Unit**
	THOMAS GYORFI	2435

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/09/2016	08/24/2017	03/19/2018						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						

Trend Micro, Inc.
EX1006-70

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	12841	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
L2	12957	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
L3	5616	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
L4	8877	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
L5	26580	(L1 L2 L3 L4) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2018/03/19 09:22
L6	3682	giuliani.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:51
L7	719	bizzarri.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:51
L8	99	voltattorni.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52
L9	7205	mayr.in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52
L10	506	(l6 l7 l8 l9) and (marco benedetto johannes).in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52
L11	1	l10 and l5	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2018/03/19 09:52

S1	1	("20150215335").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:21
S2	0	("2014033132220150020202").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:22
S3	2	(("20140331322") or ("20150020202")).PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:22
S4	10085	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:28
S5	10411	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S6	4638	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S7	7140	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S8	24673	(S4 S5 S6 S7) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S9	5	("20050108562" | "20110145924" | "20120255013" | "20120255018" | "8510596").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:31
S10	10085	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S11	10411	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S12	4638	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S13	7140	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S14	24673	(S10 S11 S12 S13) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52

S15	17	S14 and stack adj walk$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S16	55	S14 and base adj pointer	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
S17	498	S14 and virtual adj memory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S18	43	S17 and (S15 S16)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S19	70	(S15 S16)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S20	2	(S15 and S16)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S21	1	S18 and S20	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
S22	21	ntallocatevirtualmemory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S23	19	ntprotectvirtualmemory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S24	27	ntcreateprocess	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S25	5	ntcreateprocessex	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
S26	0	ntcreateuseriprocess	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:58

S27	14	ldrloaddll	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:58
S28	2	S22 S23 S24 S25 S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 17:58
S29	2	(S22 S23 S24 S25) or (S22 S23 S25 S27) or (S22 S24 S25 S27) or (S23 S24 S25 S27)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 17:59
S30	2	(S22 S23 S24) or (S22 S23 S25) or (S22 S23 S27) or (S23 S24 S25) or (S23 S24 S27) or (S24 S25 S27)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 18:00
S31	5	("20050108562" | "20110145924" | "20120255013" | "20120255018" | "8510596").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 18:12
S32	2	S31 and (S22 S23 S24 S25 S27)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 18:12
S33	1	("20120255018").PN.	US-PGPUB; USPAT	OR	OFF	2017/08/24 13:00
S34	11779	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S35	11993	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S36	5257	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S37	8224	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S38	26121	(S34 S35 S36 S37) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
S39	674	S38 and (hook shim)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:03

S40	308	S39 and ((hook shim) same (process memory space))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:03
S41	94	S39 and ((hook shim) same (monitor$3 with (process memory space)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:04

EAST Search History (Interference)

<This search history is empty>

3/19/2018 10:32:00 AM
C:\Users\tgyorfi\Documents\EAST\Workspaces\14606604.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14606604	GIULIANI ET AL.
	Examiner	**Art Unit**
	THOMAS GYORFI	2435

CPC- SEARCHED

Symbol	Date	Examiner
H04L 63/1408, 1441	12/9/16	TAG
G06F 21/52, 554	12/9/16	TAG
H04L 63/1408, 1441	8/24/17	TAG
G06F 21/52, 554	8/24/17	TAG
H04L 63/1408, 1441	3/19/18	TAG
G06F 21/52, 554	3/19/18	TAG

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES

Search Notes	Date	Examiner
EAST search	12/9/16	TAG
NPL search (Google)	12/9/16	TAG
EAST search (updated)	8/24/17	TAG
EAST search (updated)	3/19/18	TAG

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Trend Micro, Inc.
EX1006-76

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
14/606,604	01/27/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	x $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	x $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT

02/28/2018	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x $50 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	x $230 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
VENESSA JONES

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14/606,604	Filing Date	2015-01-27	Docket Number (if applicable)	04584.0117USU1	Art Unit	2435
First Named Inventor	Marco Giuliani			Examiner Name	GYORFI, THOMAS		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☒ Other Extension of Time

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132725

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

Trend Micro, Inc.
EX1006-78

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Christopher R. Stanton/	Date (YYYY-MM-DD)	2018-02-28
Name	Christopher R. Stanton	Registration Number	75801

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0117USU1

Application Number: 14/606,604 | Filed: 01-27-2015

For: DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

Art Unit: 2435 | Examiner: GYORFI, THOMAS

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1,400.00
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132725.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 75,801.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Christopher R. Stanton/
Signature

February 28, 2018
Date

Christopher R. Stanton
Typed or printed name

303.357.1647
Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT
Conf. No. 7326

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Giuliani et al.	Examiner:	GYORFI, THOMAS A.
Serial No.:	14/606,604	Group Art Unit:	2435
Filed:	January 27, 2015	Docket No.:	04584.0117USU1
Title:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS		

AMENDMENT & RESPONSE TO FINAL OFFICE ACTION

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Final Office Action mailed August 31, 2017, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Trend Micro, Inc.
EX1006-83

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer-implemented method comprising:

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

invoking one of the plurality of functions as a result of receiving a call from an application programming instance;

executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when, during the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

2. (Original) The method according to claim 1, wherein performing the memory check occur before an address of an originating caller function is reached.

3. (Original) The method according to claim 1, further comprising:

identifying an address associated with the invoked function; and

when the address of the invoked function address is found in a cache, preventing execution of a payload for the invoked function.

4. (Original) The method according to claim 1, wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function.

5. (Original) The method according to claim 1, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

6. (Original) The method according to claim 1, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

7. (Original) The method according to claim 1, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

8. (Original) The method according to claim 6, wherein performing the one or more memory checks comprises evaluating state information associated with a cache entry for the hooked function.

9. (Original) The method according to claim 8, wherein when an address of the invoked function is found in a cache, preventing execution of a payload for the invoked function.

10. (Currently Amended) A system comprising:

at least one memory; and

at least one processor connected with the memory configured to perform operation of:

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

invoking one of the plurality of functions as a result of receiving a call from an application programming instance;

executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, one or more memory checks to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when, during the performing of the one or more memory checks detect at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, the method further comprising preventing execution of a payload for the invoked function.

11. (Original) The system according to claim 10, wherein the performing of the one or more memory checks occur before an address of an originating caller function is reached.

12. (Original) The system according to claim 10, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

13. (Original) The system according to claim 10, wherein the executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function.

14. (Original) The system according to claim 10, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

15. (Original) The system according to claim 10, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, and wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

16. (Original) The system according to claim 10, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

17. (Original) The system according to claim 15, wherein performing of the memory checks comprises evaluating state information associated with a cache entry for the hooked function.

18. (Original) The system according to claim 17, wherein when an address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

19. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

invoking one of the plurality of functions as a result of receiving a call from an application programming instance;

executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack,

a return address is detected as being inside a virtual memory area, and

a low level user mode function is attempted to be executed in a cache, wherein the cache is evaluated for an address of the invoked function, and

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function.

20. (Original) The computer-readable storage device according to claim 19, wherein performing of the memory check to determine if code execution is attempted from non-executable memory, the base pointer is identified as being invalid, an invalid stack return address is identified, execution of a return-oriented programming technique is attempted, the base pointer is detected as being outside a current thread stack, and the return address is detected as being inside a virtual memory area, occurs before an address of the invoked function is reached, and

wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the final Office Action dated August 31, 2017, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claims 1-6, 8-15, and 17-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam (U.S. Publ. No. 2012/0255018; hereinafter "Sallam") in view of Yeap (U.S. Publ. No. 2007/0016914; hereinafter "Yeap"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam in view of Yeap as applied to claims 1 and 10, and further in view of Kolsek et al. (U.S. Publ. No. 2011/0145924; hereinafter "Kolsek") in view of Khazan et al. (U.S. Publ. No. 2005/0108562; hereinafter "Khazan").

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 10, and 19 have been amended. No claims have been canceled or added. Therefore, claims 1-20 remain present for examination.

Claim Rejections Under § 103:

Claims 1-6, 8-15, and 17-20

Claims 1-6, 8-15, and 17-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam in view of Yeap. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Trend Micro, Inc.
EX1006-89

Aspects of the present disclosure relate to systems and methods for monitoring a memory space of a process. In some aspects, monitoring the memory space includes execution of a stack walk, which is initiated upon invocation of a function call from an application program or application program interface.

Sallam is different. Sallam generally relates to a security agent configured to execute on the electronic device at a level below all of the operating systems of the electronic device accessing the memory or a storage of the electronic device. As part of the disclosure, Sallam discusses instances where a security agent can access the stack "to determine the order of calls made by different processes or applications of operating system 212." Sallam at [0060]. Sallam's disclosure of accessing the stack, however, is distinguishable from the current application because the stack walk of the present disclosure occurs as a result of a call from a programming application (e.g., an application that may be malicious). To clarify this distinction, Applicants have amended claim 1 to include "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space."

In contrast to the present technology, Yeap does not allow software to cause system resources to be manipulated (e.g., enter the kernel mode) as a result of a system call from an API, prior to performing a security check. Rather, Yeap provides a scheme whereby an API interception application 106 that "can intercept all user mode call threads directed to the kernel mode API 114." Yeap at [0024]. As evident in Fig. 1, the API interception application of Yeap is prior to the kernel mode. It is thus, the intention of Yeap to prevent calls that require interaction with the kernel to be intercepted and analyzed for malicious software. Indeed, Yeap explicitly states as much, noting: "[I]n one implementation, the API interception application is part of a security system. . . . The security system can examine intercepted calls **to prevent the malicious software from being transported into the kernel** layer using the call command." Yeap at [0026] (emphasis added). As such, Yeap would never allow the execution of a stack walk, which is a system process, in response to a function call by an application, as the claims require.

The Office appears to interpret Yeap paragraphs [0024]-[0028] to interpret that a security evaluation is passed at the kernel level. Office Action at 4 (noting: "A User Mode API

Interception Application . . . inserts one or more hooks into said user application to monitor their use of one or more system call functions, **which relays the call information to a kernel mode component that performs the security evaluation**: paragraphs 0024-0028, and Figure 1."(emphasis added)). Applicants respectfully disagree with the Office's interpretation of Yeap. In particular, Fig. 1 of Yeap explicitly provides that the API interception application 106 is in the user mode:

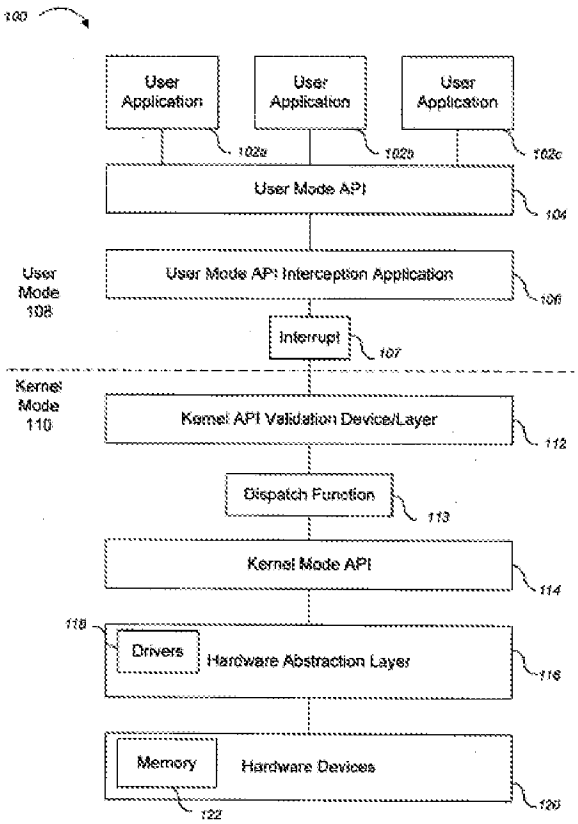


FIG. 1

As the API 106 performs the security check and creates an interrupt 107 prior to the call entering the kernel mode, Applicants submit that no system actions are performed under Yeap as a result of receiving a call.

In short, whereas Yeap interrupts a system call from an API prior to entering the kernel mode, aspects of the technology execute a stack walk upon an invocation of a system call from an API. To clarify this distinction, Applicants have amended claim 1 to include "invoking one of

the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space." Thus, claim 1 is allowable over Sallam in view of Yeap.

For at least similar reasons, independent claim 10 is also allowable. Claim 10 recites, *inter alia*, "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space." Thus, claim 10 is allowable for at least similar reasons as discussed with respect to independent claim 1.

Independent claim 19 is also allowable for at least similar reasons. Claim 19 recites, *inter alia*, ""invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space." Thus, claim 19 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1, 10, and 19 were allowable over the cited Sallam. All other claims, i.e., claims 2-6, 8-15, and 17-20, depend from one of allowable claims 1, 10, or 19 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 1-6, 8-15, and 17-20.

<u>Claims 7 and 16</u>

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sallam in view of Yeap as applied to claims 1 and 10, and further in view of Kolsek in view of Khazan. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct.

Trend Micro, Inc.
EX1006-92

1727, 1741 (2007). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

For at least the reasons discussed above, claim 1 is allowable over Sallam in view of Yeap. Applicants respectfully submit that Kolsek fails to compensate for the deficiencies of Sallam's and/or Yeap deficiencies. Kolsek generally relates to observing the calls of system and application functions, and the arguments of such calls, which play a key role in loading executable files, and detects that a computer program or operating system either has tried, is trying or will try to load or execute an executable file from the current working directory. Kolsek, however, fails to teach or suggest at least "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space," as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Sallam, Yeap, and Kolsek.

Khazan fails as well. Khazan generally relates to automatic detection of malicious code by verifying that an application executes in accordance with a model defined using calls to a predetermined set of targets, such as external routines. A model is constructed using a static analysis of a binary form of the application, and is comprised of a list of calls to targets, their invocation and target locations, and possibly other call-related information. Khazan, however, fails to teach or suggest at least "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space," as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Sallam, Yeap, Kolsek, and Khazan.

For at least similar reasons, independent claim 10 is also allowable. Claim 10 recites, *inter alia*, "invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space." Thus, claim 10 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 10 are allowable over the cited references. Claims 7 and 16 depend from one of allowable claims 1 or 10 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 7 and 16.

Trend Micro, Inc.
EX1006-94

CONCLUSION

This Amendment fully responds to the Office Action mailed on August 31, 2017. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicants believe the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Petition for Extension of Time and a Request for Continued Examination. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: February 28, 2018

/Christopher R. Stanton/

Christopher R. Stanton, Reg. No. 75,801
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1647

23552
PATENT TRADEMARK OFFICE

Trend Micro, Inc.
EX1006-95

Electronic Patent Application Fee Transmittal

Application Number:	14606604
Filing Date:	27-Jan-2015
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Filer:	Christopher R. Stanton/Eileen Ellefsen
Attorney Docket Number:	04584.0117USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
RCE- 1st Request	1801	1	1300	1300
		Total in USD ($)		**2700**

Electronic Acknowledgement Receipt

EFS ID:	31924693
Application Number:	14606604
International Application Number:	
Confirmation Number:	7326
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Customer Number:	23552
Filer:	Christopher R. Stanton/Eileen Ellefsen
Filer Authorized By:	Christopher R. Stanton
Attorney Docket Number:	04584.0117USU1
Receipt Date:	28-FEB-2018
Filing Date:	27-JAN-2015
Time Stamp:	18:47:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2700
RAM confirmation Number	030118INTEFSW18482800
Deposit Account	132725
Authorized User	Eileen Ellefsen

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	04584_0117USU1_RCE.PDF	1349907 aa540f387843ac701c2dd91e25626d618f7b8b73	no	3
Warnings:					
Information:					
2	Extension of Time	04584_0117USU1_EOT.PDF	164753 f83c916303c59a8d62bf416e237fdb72480a2c32	no	2
Warnings:					
Information:					
3		2018-02-28_Response_04584_0117USU1.PDF	171330 31e9bcd482ca924eceefa05b1b71d6d537fd5670	yes	13

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	13

Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32637 63258b6db16651c088e8b135de79d96a6a504879	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1718627	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1	7326

23552 7590 08/31/2017
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
08/31/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Trend Micro, Inc.
EX1006-101

Office Action Summary	Application No. 14/606,604	Applicant(s) GIULIANI ET AL.	
	Examiner Thomas Gyorfi	Art Unit 2435	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 6/16/17.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) 1-20 is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Trend Micro, Inc.
EX1006-102

DETAILED ACTION

1. Claims 1-20 remain for examination. The amendment filed amended 6/16/17 claims 1, 10, and 19. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

2. Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claim 1-6, 8-15, and 17-20 are rejected under 35 U.S.C. 103 as being unpatentable over Salaam (U.S. Patent Publication 2012/0255018) in view of Yeap (U.S. Patent Publication 2007/0016914).

Regarding claims 1, 10, and 19:

Salaam discloses a computer-implemented method, system, and computer storage device comprising: monitoring a memory space of a process for execution of at least one of a plurality of functions (paragraph 0077); executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space (paragraph 0060); and performing, during the executing of the stack walk processing, at

least one memory check to detect suspicious behavior (Ibid), wherein an alert of suspicious behavior is triggered when, during the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating (pointer and virtual memory conditions at paragraphs 0239-0242). Per claim 10, Salaam further discloses a memory and processor (paragraphs 0045-0046).

Salaam appears to be silent regarding wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space. However, Yeap discloses a related invention for monitoring the memory space of an process for execution comprising this limitation (a User Mode API Interception Application, running in the same user mode memory space as the user applications, inserts one or more hooks into said user applications to monitor their use of one or more system call functions, which relays the call information to a kernel mode component that performs the security evaluation: paragraphs 0024-0028, and Figure 1). It would have been obvious to install hooks into the processes monitored by Salaam, as this approach can be used to detect if malware has hijacked a process and thwart its execution (Yeap, Ibid, particularly paragraphs 0026-0028).

Regarding claims 2 and 11:

Salaam further discloses wherein performing the memory check occur before an address of an originating caller function is reached (paragraph 0224).

Regarding claims 3 and 12:

Salaam further discloses further comprising: identifying an address associated with the invoked function (paragraph 0067); and when the address of the invoked function address is found in a cache, preventing execution of a payload for the invoked function (paragraphs 0138 & 0211).

Regarding claims 4 and 13:

Salaam further discloses wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function (paragraph 0060).

Regarding claims 5 and 14:

Salaam further discloses wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function (paragraphs 0039 & 0042).

Regarding claims 6 and 15:

Salaam further discloses wherein the monitoring further comprises applying,

upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function (paragraphs 0039, 0049, & 0090), wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function (Ibid, and also paragraph 0060).

Regarding claims 8 and 17:

Salaam further discloses wherein performing the one or more memory checks comprises evaluating state information associated with a cache entry for the hooked function (paragraphs 0090, 0193, 0207, 0214, & 0269).

Regarding claims 9 and 18:

Salaam further discloses wherein when an address of the invoked function is found in a cache, preventing execution of a payload for the invoked function (paragraphs 0138 & 0211).

Regarding claim 20:

Salaam further discloses wherein performing of the memory check to determine if code execution is attempted from non-executable memory, the base pointer is identified as being invalid (paragraph 0276), an invalid stack return address is identified (paragraphs 0049 & 0060), execution of a return-oriented programming technique is attempted (paragraph 0117), the base pointer is detected as being outside a current

thread stack (paragraphs 0049 & 0060), and the return address is detected as being inside a virtual memory area (paragraphs 0239-0240), occurs before an address of the invoked function is reached (paragraph 0224), and wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing (paragraphs 0039, 0207, and 0224).

5. Claims 7 & 16 are rejected under 35 U.S.C. 103 as being unpatentable over Salaam in view of Yeap as applied to claims 1 & 10 above, and further in view of Kolsek (U.S. Patent Publication 2011/0145924) in view of Khazan (U.S. Patent Publication 2005/0108562).

Regarding claims 7 and 16:

Although Salaam discloses an open-ended list of functions that can be monitored by his invention, explicitly including wherein the plurality of functions comprises the NtAllocateVirtualMemory and NtProtectVirtualMemory functions (paragraph 0283), nevertheless Salaam and Yeap are silent regarding the NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function. However, Kolsek discloses a related invention for preventing the execution of malware by *inter alia* monitoring and intercepting function calls including NTCreateProcess, NtCreateUserIProcess, and LdrLoadDLL (paragraphs 0049-0065). It would have been obvious to modify Salaam to also monitor these particular functions,

as these functions were known to present a vulnerability that would allow malicious hackers to plant malware in a way that was not previously detectable by the prior art (Kolsek, paragraphs 0014-0020 & 0038).

Neither Salaam, Yeap, nor Kolsek names the NTCreateProcessEx function. However, Khazan discloses a similar invention for detecting malware wherein an analyzer is triggered upon invocation of NTCreateProcessEx (Khazan, paragraph 0076). It would have been obvious for Salaam to also monitor NTCreateProcessEx, as this technique allows for detection of both known and unknown threats (Khazan, paragraphs 0009-0010).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: U.S. Patent Publications 2009/0049550 (Shevchenko) and 2013/0198527 (Lu).

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 10:00am - 6:30pm Monday - Friday.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on (571) 272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thomas Gyorfi/
Examiner, Art Unit 2435
8/24/17

/JOSEPH P. HIRL/
Supervisory Patent Examiner, Art Unit 2435

Notice of References Cited	Application/Control No. 14/606,604	Applicant(s)/Patent Under Reexamination GIULIANI ET AL.	
	Examiner Thomas Gyorfi	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2013/0198527 A1	08-2013	Lu; Zhou	G06F9/445	713/189
*	B	US-2009/0049550 A1	02-2009	Shevchenko; Sergei	G06F21/56	726/23
*	C	US-2007/0016914 A1	01-2007	Yeap; Yuen-Pin	G06F21/554	719/328
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1006-111

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14606604	GIULIANI ET AL.
	Examiner	**Art Unit**
	THOMAS GYORFI	2435

CPC- SEARCHED

Symbol	Date	Examiner
H04L 63/1408, 1441	12/9/16	TAG
G06F 21/52, 554	12/9/16	TAG
H04L 63/1408, 1441	8/24/17	TAG
G06F 21/52, 554	8/24/17	TAG

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES

Search Notes	Date	Examiner
EAST search	12/9/16	TAG
NPL search (Google)	12/9/16	TAG
EAST search (updated)	8/24/17	TAG

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Trend Micro, Inc.
EX1006-112

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	("20120255018").PN.	US-PGPUB; USPAT	OR	OFF	2017/08/24 13:00
L2	11779	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
L3	11993	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
L4	5257	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
L5	8224	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
L6	26121	(L2 L3 L4 L5) and @ad< "20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/08/24 13:02
L7	674	l6 and (hook shim)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:03
L8	308	l7 and ((hook shim) same (process memory space))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:03
L9	94	l7 and ((hook shim) same (monitor$3 with (process memory space)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	OFF	2017/08/24 13:04

8/24/2017 1:40:44 PM
C:\Users\tgyorfi\Documents\EAST\Workspaces\14606604.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14606604	GIULIANI ET AL.
	Examiner	**Art Unit**
	THOMAS GYORFI	2435

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/09/2016	08/24/2017							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

Trend Micro, Inc.
EX1006-114

PATENT
Conf. No. 7326

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Giuliani et al.	Examiner:	Gyorfi, Thomas A.
Serial No.:	14/606,604	Group Art Unit:	2435
Filed:	January 27, 2015	Docket No.:	04584.0117USU1
Title:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS		

AMENDMENT & RESPONSE TO NON-FINAL OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Non-Final Office Action mailed December 16, 2016, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Trend Micro, Inc.
EX1006-115

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer-implemented method comprising:

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when, during the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

2. (Original) The method according to claim 1, wherein performing the memory check occur before an address of an originating caller function is reached.

3. (Original) The method according to claim 1, further comprising:

identifying an address associated with the invoked function; and

when the address of the invoked function address is found in a cache, preventing execution of a payload for the invoked function.

Trend Micro, Inc.
EX1006-116

4. (Original) The method according to claim 1, wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function.

5. (Original) The method according to claim 1, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

6. (Original) The method according to claim 1, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

7. (Original) The method according to claim 1, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

8. (Original) The method according to claim 6, wherein performing the one or more memory checks comprises evaluating state information associated with a cache entry for the hooked function.

9. (Original) The method according to claim 8, wherein when an address of the invoked function is found in a cache, preventing execution of a payload for the invoked function.

10. (Currently Amended) A system comprising:

at least one memory; and

at least one processor connected with the memory configured to perform operation of:

Trend Micro, Inc.
EX1006-117

monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, one or more memory checks to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when, during the performing of the one or more memory checks detect at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, the method further comprising preventing execution of a payload for the invoked function.

11. (Original) The system according to claim 10, wherein the performing of the one or more memory checks occur before an address of an originating caller function is reached.

12. (Original) The system according to claim 10, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

13. (Original) The system according to claim 10, wherein the executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function.

14. (Original) The system according to claim 10, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

15. (Original) The system according to claim 10, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, and wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

16. (Original) The system according to claim 10, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

17. (Original) The system according to claim 15, wherein performing of the memory checks comprises evaluating state information associated with a cache entry for the hooked function.

18. (Original) The system according to claim 17, wherein when an address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

19. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

monitoring a memory space of a process for execution of at least one <u>monitored function</u> of a plurality of functions<u>, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space</u>;

Trend Micro, Inc.
EX1006-119

executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack,

a return address is detected as being inside a virtual memory area, and

a low level user mode function is attempted to be executed in a cache, wherein the cache is evaluated for an address of the invoked function, and

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function.

20. (Original) The computer-readable storage device according to claim 19, wherein performing of the memory check to determine if code execution is attempted from non-executable memory, the base pointer is identified as being invalid, an invalid stack return address is identified, execution of a return-oriented programming technique is attempted, the base pointer is detected as being outside a current thread stack, and the return address is detected as being inside a virtual memory area, occurs before an address of the invoked function is reached, and

wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing.

Trend Micro, Inc.
EX1006-120

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the non-final Office Action dated December 16, 2016, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claims 1-6, 8-15, and 17-20 were rejected under 35 U.S.C. § 102(a)(1) and 35 U.S.C. § 102(a)(2) as allegedly anticipated by Salaam (U.S. Publ. No. 2012/0255018; hereinafter "Sallam"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Salaam as applied to claims 1 and 10, and further in view of Kolsek et al. (U.S. Publ. No. 2011/0145924; hereinafter "Kolsek") in view of Khazan et al. (U.S. Pat./Appl. Ser./Publ. No. 2005/0108562; hereinafter "Khazan").

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 10, and 19 have been amended and no claims have been canceled or added. Therefore, claims 1-20 remain present for examination.

Claim Rejections under 35 U.S.C. § 102:

Claims 1-6, 8-15, and 17-20 were rejected under 35 U.S.C. § 102(a)(1) and 35 U.S.C. § 102(a)(2) as allegedly anticipated by Salaam. Applicants respectfully traverse this rejection because either the Examiner failed to state a *prima facie* case of anticipation or the current amendments to the claims now render the Examiner's arguments moot. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Mashinenfabrik GmbH v. Am. Hoist & Derrick Co.,* 730 F.2d 1452, 1458 (Fed. Cir. 1984); *see also,* MPEP § 2131. Applicants submit that the cited reference does not disclose all of the elements of the rejected claims.

Aspects of the present disclosure relate to systems and methods for monitoring a memory space of a process. In some aspects, monitoring the memory space of the process comprises loading a component for evaluating the at least one monitored function in the memory space.

Sallam generally relates to a security agent configured to execute on the electronic device at a level below all of the operating systems of the electronic device accessing the memory or a

Trend Micro, Inc.
EX1006-121

storage of the electronic device may be further configured to: (i) access one or more security rules to determine a criteria by which an attempted access involving a transfer of content between the memory and the storage of an electronic device will be trapped; (ii) if the criteria is met, trap, at a level below all of the operating systems of the electronic device, attempted access of data between memory and storage of an electronic device; and (iii) analyze, at a level below all of the operating systems of the electronic device, information associated with the attempted access to determine if the attempted access was affected by malware.

Turning now to the claims, Sallam fails to teach or suggest at least "monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space," as recited in independent claim 1. To be sure, there is no teaching that any of Sallam's agents are loaded into the monitored memory space of a process. Thus, claim 1 is allowable over Sallam.

For at least similar reasons, independent claim 10 is also allowable. Claim 10 recites, *inter alia*, "monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space." Thus, claim 10 is allowable for at least similar reasons as discussed with respect to independent claim 1.

Independent claim 19 is also allowable for at least similar reasons. Claim 19 recites, *inter alia*, "monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space. Thus, claim 10 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1, 10, and 19 were allowable over the cited Sallam. All other claims, i.e., claims 2-6, 8-15, and 17-20, depend from one of allowable claims 1, 10, or 19 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 1-6, 8-15, and 17-20.

Trend Micro, Inc.
EX1006-122

Claim Rejections Under § 103:

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Salaam as applied to claims 1 and 10, and further in view of Kolsek in view of Khazan. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

For at least the reasons discussed above, claim 1 is allowable over Sallam. Applicants respectfully submit that Kolsek fails to compensate for Sallam's deficiencies. Kolsek generally relates to observing the calls of system and application functions, and the arguments of such calls, which play a key role in loading executable files, and detects that a computer program or operating system either has tried, is trying or will try to load or execute an executable file from the current working directory. Kolsek, however, fails to teach or suggest at least "monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space," as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Sallam and Kolsek.

Khazan fails to compensate for the deficiencies of Sallam and Kolsek. Khazan generally relates to automatic detection of malicious code by verifying that an application executes in accordance with a model defined using calls to a predetermined set of targets, such as external routines. A model is constructed using a static analysis of a binary form of the application, and is comprised of a list of calls to targets, their invocation and target locations, and possibly other call-related information. Khazan, however, fails to teach or suggest at least "monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating

the at least one monitored function in the memory space," as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Sallam, Kolsek, and Khazan.

For at least similar reasons, independent claim 10 is also allowable. Claim 10 recites, *inter alia*, "monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space." Thus, claim 10 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 10 are allowable over the cited references. Claims 7 and 16 depend from one of allowable claims 1 or 10 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 7 and 16.

Trend Micro, Inc.
EX1006-124

CONCLUSION

This Amendment fully responds to the Office Action mailed on December 16, 2016. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicants believe the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Petition for Extension of Time. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: June 16, 2017

/Andrew T. Pouzeshi/

Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

Trend Micro, Inc.
EX1006-125

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0117USU1

Application Number: 14/606,604

Filed: January 27, 2015

For: DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

Art Unit: 2435

Examiner: GYORFI, THOMAS A.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1,400.00
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☑ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132725.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 67672.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Andrew T. Pouzeshi/
Signature

June 16, 2017
Date

Andrew T. Pouzeshi
Typed or printed name

303.357.1639
Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14606604
Filing Date:	27-Jan-2015
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0117USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
			Total in USD ($)	**1400**

Electronic Acknowledgement Receipt

EFS ID:	29521963
Application Number:	14606604
International Application Number:	
Confirmation Number:	7326
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0117USU1
Receipt Date:	16-JUN-2017
Filing Date:	27-JAN-2015
Time Stamp:	13:46:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1400
RAM confirmation Number	061617INTEFSW13473600
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2017-06-16-RespNFOA-of-121616-04584-0117USU1.PDF	134727 f66c5d236da28cb0d0b74deb5db5773d9643e16c	yes	11

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	11

Warnings:

Information:

2	Extension of Time	2017-06-16-EOT-04584-0117USU1.PDF	194564 a212b0be9ee4d5ec3e55479482d164c87b2a6bad	no	2

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	31050 11d66a14cdf385497d1482f8219cf865bb4a4dd6	no	2

Warnings:

Information:

Total Files Size (in bytes):	360341

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
14/606,604	01/27/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	x $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	x $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT

06/16/2017	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	x $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

SLIE
DESHONNE T. MARTINO

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1	7326

23552 7590 12/16/2016
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
12/16/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Trend Micro, Inc.
EX1006-134

Office Action Summary	Application No. 14/606,604	Applicant(s) GIULIANI ET AL.	
	Examiner Thomas Gyorfi	Art Unit 2435	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 1/27/15.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) 1-20 is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 5/15/15.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Trend Micro, Inc.
EX1006-135

DETAILED ACTION

1. Claims 1-20 are presented for examination. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 1/27/15 has been considered by the Examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

4. Claim(s) 1-6, 8-15, and 17-20 are rejected under 35 U.S.C. 102(a)(1) and 35 U.S.C. 102(a)(2) as being anticipated by Salaam (U.S. Patent Publication 2012/0255018).

Regarding claims 1, 10, and 19:

Salaam discloses a computer-implemented method, system, and computer storage device comprising: monitoring a memory space of a process for execution of at

least one of a plurality of functions (paragraph 0077); executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space (paragraph 0060); and performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior (Ibid), wherein an alert of suspicious behavior is triggered when, during the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating (pointer and virtual memory conditions at paragraphs 0239-0242). Per claim 10, Salaam further discloses a memory and processor (paragraphs 0045-0046).

Regarding claims 2 and 11:

Salaam further discloses wherein performing the memory check occur before an address of an originating caller function is reached (paragraph 0224).

Regarding claims 3 and 12:

Salaam further discloses further comprising: identifying an address associated with the invoked function (paragraph 0067); and when the address of the invoked

function address is found in a cache, preventing execution of a payload for the invoked function (paragraphs 0138 & 0211).

Regarding claims 4 and 13:

Salaam further discloses wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function (paragraph 0060).

Regarding claims 5 and 14:

Salaam further discloses wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function (paragraphs 0039 & 0042).

Regarding claims 6 and 15:

Salaam further discloses wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function (paragraphs 0039, 0049, & 0090), wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function (Ibid, and also paragraph 0060).

Regarding claims 8 and 17:

Salaam further discloses wherein performing the one or more memory checks comprises evaluating state information associated with a cache entry for the hooked function (paragraphs 0090, 0193, 0207, 0214, & 0269).

Regarding claims 9 and 18:

Salaam further discloses wherein when an address of the invoked function is found in a cache, preventing execution of a payload for the invoked function (paragraphs 0138 & 0211).

Regarding claim 20:

Salaam further discloses wherein performing of the memory check to determine if code execution is attempted from non-executable memory, the base pointer is identified as being invalid (paragraph 0276), an invalid stack return address is identified (paragraphs 0049 & 0060), execution of a return-oriented programming technique is attempted (paragraph 0117), the base pointer is detected as being outside a current thread stack (paragraphs 0049 & 0060), and the return address is detected as being inside a virtual memory area (paragraphs 0239-0240), occurs before an address of the invoked function is reached (paragraph 0224), and wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing (paragraphs 0039, 0207, and 0224).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 7 & 16 are rejected under 35 U.S.C. 103 as being unpatentable over Salaam as applied to claims 1 & 10 above, and further in view of Kolsek (U.S. Patent Publication 2011/0145924) in view of Khazan (U.S. Patent Publication 2005/0108562).

Regarding claims 7 and 16:

Although Salaam discloses an open-ended list of functions that can be monitored by his invention, explicitly including wherein the plurality of functions comprises the NtAllocateVirtualMemory and NtProtectVirtualMemory functions (paragraph 0283), nevertheless Salaam is silent regarding the NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function. However, Kolsek discloses a related invention for preventing the execution of malware by *inter alia* monitoring and intercepting function calls including NTCreateProcess, NtCreateUserIProcess, and LdrLoadDLL (paragraphs 0049-0065). It would have been obvious to modify Salaam to also monitor these particular functions, as these functions were known to present a vulnerability that would allow malicious

hackers to plant malware in a way that was not previously detectable by the prior art (Kolsek, paragraphs 0014-0020 & 0038).

Neither Salaam nor Kolsek names the NTCreateProcessEx function. However, Khazan discloses a similar invention for detecting malware wherein an analyzer is triggered upon invocation of NTCreateProcessEx (Khazan, paragraph 0076). It would have been obvious for Salaam to also monitor NTCreateProcessEx, as this technique allows for detection of both known and unknown threats (Khazan, paragraphs 0009-0010).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: U.S. Patent 8,037,526 (Satish); and U.S. Patent Publications 2011/0289586 (Kc), 2007/0089088 (Borde), and 2006/0230388 (Hatlelid).

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 10:00am - 6:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on (571) 272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thomas Gyorfi/
Examiner, Art Unit 2435
12/9/16

Notice of References Cited	Application/Control No. 14/606,604	Applicant(s)/Patent Under Reexamination GIULIANI ET AL.	
	Examiner Thomas Gyorfi	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8,037,526 B1	10-2011	Satish; Sourabh	G06F21/52	711/6
*	B	US-2011/0289586 A1	11-2011	Kc; Gaurav S.	G06F21/566	726/24
*	C	US-2007/0089088 A1	04-2007	Borde; Shrikrishna V.	G06F21/52	717/106
*	D	US-2006/0230388 A1	10-2006	Hatlelid; Kristjan E.	G06F21/52	717/127
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1006-143

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7326

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/606,604	01/27/2015 RULE	726	2435	04584.0117USU1

APPLICANTS
WEBROOT INC., Broomfield, CO;

INVENTORS
Marco Giuliani, Bastia Umbra (PG), ITALY;
Marco Bizzarri, Sassoferrato (AN), ITALY;
Benedetto Voltattorni, San Benedetto del Tronto (AP), ITALY;
Johannes Mayr, Linz, AUSTRIA;

**** CONTINUING DATA ***************************
This appln claims benefit of 61/931,772 01/27/2014

**** FOREIGN APPLICATIONS ****************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
02/06/2015

Foreign Priority claimed	☐ Yes ☑ No	☐ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	☐ Yes ☑ No		ITALY	4	20	3
Verified and Acknowledged	/THOMAS A GYORFI/ Examiner's Signature	Initials				

ADDRESS
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903
UNITED STATES

TITLE
DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

FILING FEE RECEIVED		
730	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Trend Micro, Inc.
EX1006-144

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14606604	GIULIANI ET AL.
	Examiner	**Art Unit**
	THOMAS GYORFI	2435

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/09/2016								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Trend Micro, Inc.
EX1006-145

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14606604
Filing Date	2015-01-27
First Named Inventor	Marco Giuliani
Art Unit	2431
Examiner Name	Not assigned
Attorney Docket Number	04584.0117USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.A.G/	1	8510596		2013-08-13	Gupta et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.A.G/	1	20120255018		2012-10-04	Sallam	
/T.A.G/	2	20120255013		2012-10-04	Sallam	
/T.A.G/	3	20110145924		2011-06-16	Kolsek et al.	
/T.A.G/	4	20050108562		2005-05-19	Khazan et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

Trend Micro, Inc.
EX1006-146

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14606604
	Filing Date	2015-01-27
	First Named Inventor	Marco Giuliani
	Art Unit	2431
	Examiner Name	Not assigned
	Attorney Docket Number	04584.0117USU1

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/T.A.G/	1	International Search Report and Written Opinion for International Application No. PCT/US15/13111, mailed April 17, 2015, 15 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/THOMAS A GYORFI/	Date Considered	12/09/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14606604
	Filing Date	2015-01-27
	First Named Inventor	Marco Giuliani
	Art Unit	2431
	Examiner Name	Not assigned
	Attorney Docket Number	04584.0117USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2015-05-15
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	10085	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
L3	10411	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
L4	4638	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
L5	7140	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
L6	24673	(L2 L3 L4 L5) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
L7	17	L6 and stack adj walk$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
L8	55	L6 and base adj pointer	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:52
L9	498	L6 and virtual adj memory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
L10	43	l9 and (l7 l8)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
L11	70	(l7 l8)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53

L12	2	(l7 and l8)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
L13	1	l10 and l12	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:53
L14	21	ntallocatevirtualmemory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
L15	19	ntprotectvirtualmemory	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
L16	27	ntcreateprocess	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
L17	5	ntcreateprocessex	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:57
L18	0	ntcreateuseriprocess	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:58
L19	14	ldrloaddll	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 17:58
L20	2	l14 l15 l16 l17 l19	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 17:58
L21	2	(l14 l15 l16 l17) or (l14 l15 l17 l19) or (l14 l16 l17 l19) or (l15 l16 l17 l19)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 17:59
L22	2	(l14 l15 l16) or (l14 l15 l17) or (l14 l15 l19) or (l15 l16 l17) or (l15 l16 l19) or (l16 l17 l19)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2016/12/09 18:00
L23	5	("20050108562" | "20110145924" | "20120255013" | "20120255018" | "8510596").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 18:12
L24	2	L23 and (l14 l15 l16 l17 l19)	US-PGPUB;	OR	OFF	2016/12/09

			USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB			18:12
S1	1	("20150215335").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:21
S2	0	("2014033132220150020202").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:22
S3	2	(("20140331322") or ("20150020202")).PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:22
S4	10085	h04l63/1441.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:28
S5	10411	h04l63/1408.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S6	4638	g06f21/52.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S7	7140	g06f21/554.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S8	24673	(S4 S5 S6 S7) and @ad<"20140127"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 15:29
S9	5	("20050108562" | "20110145924" | "20120255013" | "20120255018" | "8510596").PN.	US-PGPUB; USPAT	OR	OFF	2016/12/09 15:31

EAST Search History (Interference)

<This search history is empty>

12/9/2016 6:37:51 PM
C:\ Users\ tgyorfi\ Documents\ EAST\ Workspaces\ 14606604.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14606604	GIULIANI ET AL.
	Examiner	**Art Unit**
	THOMAS GYORFI	2435

CPC- SEARCHED

Symbol	Date	Examiner
H04L 63/1408, 1441	12/9/16	TAG
G06F 21/52, 554	12/9/16	TAG

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
EAST search	12/9/16	TAG
NPL search (Google)	12/9/16	TAG

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Trend Micro, Inc.
EX1006-153

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/606,604	01/27/2015	Marco Giuliani	04584.0117USU1

CONFIRMATION NO. 7326

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

PUBLICATION NOTICE

OC000000076584735

Title:DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

Publication No.US-2015-0215335-A1
Publication Date:07/30/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Trend Micro, Inc.
EX1006-154

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14606604
Filing Date	2015-01-27
First Named Inventor	Marco Giuliani
Art Unit	2431
Examiner Name	Not assigned
Attorney Docket Number	04584.0117USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8510596		2013-08-13	Gupta et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120255018		2012-10-04	Sallam	
	2	20120255013		2012-10-04	Sallam	
	3	20110145924		2011-06-16	Kolsek et al.	
	4	20050108562		2005-05-19	Khazan et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

Trend Micro, Inc.
EX1006-155

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14606604
	Filing Date	2015-01-27
	First Named Inventor	Marco Giuliani
	Art Unit	2431
	Examiner Name	Not assigned
	Attorney Docket Number	04584.0117USU1

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report and Written Opinion for International Application No. PCT/US15/13111, mailed April 17, 2015, 15 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14606604
	Filing Date	2015-01-27
	First Named Inventor	Marco Giuliani
	Art Unit	2431
	Examiner Name	Not assigned
	Attorney Docket Number	04584.0117USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2015-05-15
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: Katherine M. Kowalchyk
Merchant & Gould P.C.
P. O. Box 2903
Minneapolis, MN 55402-0903
United States of America

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)*
Applicant's or agent's file reference 4584.117WOU1	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US15/13111	International filing date *(day/month/year)* 27 January 2015 (27.01.2015)
Applicant WEBROOT INC.	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   How? Directly to the International Bureau of WIPO preferably through ePCT or on paper to, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 – 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
   - ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.
   - ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may **submit comments on an informal basis on the written opinion of the International Searching Authority** to the International Bureau. These comments will be made available to the public after international publication. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established.

   Shortly after the expiration of **18 months from the priority date, the international application will be published** by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for **entry into the national phase** before those designated Offices. In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months. For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

   Within **19 months from the priority date, the applicant may request that a supplementary international search be carried out** by a different International Searching Authority that offers this service (Rule 45*bis*.1). The procedure for requesting supplementary international search is described in the *PCT Applicant's Guide*, International Phase, paragraphs 8.006-8.032.

Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Shane Thomas Telephone No. PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/220 (July 2014)

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: Katherine M. Kowalchyk
Merchant & Gould P.C.
P. O. Box 2903
Minneapolis, MN 55402-0903
United States of America

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 17 APR 2015
Applicant's or agent's file reference 4584.117WOU1	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US15/13111	International filing date *(day/month/year)* 27 January 2015 (27.01.2015)
Applicant WEBROOT INC.	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   How? Directly to the International Bureau of WIPO preferably through ePCT or on paper to, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 – 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may **submit comments on an informal basis on the written opinion of the International Searching Authority** to the International Bureau. These comments will be made available to the public after international publication. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established.

   Shortly after the expiration of **18 months from the priority date, the international application will be published** by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for **entry into the national phase** before those designated Offices. In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months. For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

   Within **19 months from the priority date, the applicant may request that a supplementary international search be carried out** by a different International Searching Authority that offers this service (Rule 45*bis*.1). The procedure for requesting supplementary international search is described in the *PCT Applicant's Guide*, International Phase, paragraphs 8.006-8.032.

Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 Telephone No. PCT OSP: 571-272-7774

Form PCT/ISA/220 (July 2014)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 4584.117WOU1	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US15/13111	International filing date *(day/month/year)* 27 January 2015 (27.01.2015)	(Earliest) Priority Date *(day/month/year)* 27 January 2014 (27.01.2014)
Applicant WEBROOT INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      ☐ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Trend Micro, Inc.
EX1006-161

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US15/13111

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/50 (2015.01)
CPC - G06F 21/50
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) Classification(s): G06F 21/50, 21/52, 21/54, 21/55, 21/12, 21/14; H04L 29/06 (2015.01)
CPC Classification(s): G06F 21/50, 21/52, 21/54, 21/552, 21/577; H04L 63/1441, 63/1416, 63/1466

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, INPADOC); ProQuest; IEEE/IEEEXplore; Google/Google Scholar; tracking, monitoring, detecting, checking, memory, function, calls, stack; walk, intrusions, suspicious, exploit, malicious, invalid, prevent, payload

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/0255018 A1 (SALLAM, A) October 04, 2012; paragraphs [0060], [0077], [0138], [0239], [0240].	1-6, 8-15, 17-20
Y		7, 16
Y	US 2012/0255013 A1 (SALLAM, A) October 04, 2012; paragraph [0283].	7, 16
Y	US 2011/0145924 A1 (KOLSEK, M et al.) June 16, 2011; paragraphs [0052], [0056], [0058], [0065].	7, 16
Y	US 2005/0108562 A1 (KHAZAN, R et al.) May 19, 2005; paragraph [0076].	7, 16
A	US 8510596 B1 (GUPTA, S et al.) August 13, 2013; entire document.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
4 April 2015 (04.04.2015)

Date of mailing of the international search report
17 APR 2015

Name and mailing address of the ISA/
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer
Shane Thomas
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: Katherine M. Kowalchyk
Merchant & Gould P.C.
P. O. Box 2903
Minneapolis, MN 55402-0903
United States of America

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	17 APR 2015
Applicant's or agent's file reference 4584.117WOU1	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US15/13111	27 January 2015 (27.01.2015)	27 January 2014 (27.01.2014)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06F 21/50 (2015.01)
CPC - G06F 21/50

Applicant WEBROOT INC.

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	4 April 2015 (04.04.2015)	Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (January 2015)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US15/13111

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   [X] the international application in the language in which it was filed.

   [ ] a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. [ ] This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a)).

3. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. [ ] forming part of the international application as filed:

      [ ] in the form of an Annex C/ST.25 text file.

      [ ] on paper or in the form of an image file.

   b. [ ] furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. [ ] furnished subsequent to the international filing date for the purposes of international search only:

      [ ] in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      [ ] on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. [ ] In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	7, 16	YES
	Claims	1-6, 8-15, 17-20	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	NONE	NO

2. Citations and explanations:

Claims 1-6, 8-15 and 17-20 lack novelty under PCT Article 33(2) as being anticipated by US 2012/0255018 A1 to SALLAM (hereinafter "Sallam '018").

As per claim 1, Sallam '018 discloses a computer-implemented method (300) comprising: monitoring (302) a memory space of a process for execution of at least one of a plurality of functions (a security agent running underneath an operating system of an electronic device monitors access by execution of key operations (plurality of functions) to system memory; paragraph [0077]); executing (304) stack walk processing upon invocation of one of the plurality of functions in the monitored memory space (by walking through the Execution Base Pointer through the stack, previous function calls are identified providing context for the operations within memory; paragraph [0060]); and performing (304), during the executing of the stack walk processing, at least one memory check to detect suspicious behavior (by walking through the Execution Base Pointer through the stack, function calls are identified and the security agent is configured to determine whether an attempt is malicious; paragraph [0060]), wherein an alert of suspicious behavior is triggered when, during the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory (210), a base pointer is identified as being invalid (210), an invalid stack return address is identified (210), attempted execution of a return-oriented programming technique is detected (210), the base pointer is detected as being outside a current thread stack (210), and a return address is detected as being inside a virtual memory area (210) (O/S security is configured to intercept access (an alert of suspicious behavior) to memory of an electronic device such as an attempted access of pages within an address space of virtualized memory; paragraphs [0239], [0240]), wherein when an alert of suspicious behavior is triggered, preventing (310) execution of a payload for the invoked function from operating (210) (attempted access to virtualized memory address space is intercepted by O/S security, and a device security agent traps data to be sent or received (preventing execution of the payload), and scans the data payload of packets to be sent or received for evidence of malware; paragraphs [0138], [0239], [0240]).

As per claim 2, Sallam '018 discloses the method (300) according to claim 1, additionally Sallam '018 discloses, wherein performing (304) the memory check occur before an address of an originating caller function is reached (the trapping agent halts attempted resource access based on a triggered event, and the trapping agent adds additional context information about the attempt into the triggered event, such as the memory address from which the attempt originated (occur before an address of an originating caller function is reached); paragraph [0224]).

As per claim 3, Sallam '018 discloses the method (300) according to claim 1, additionally Sallam '018 discloses, further comprising: identifying (304) an address associated with the invoked function (the security agent converts the address for a function to be trapped (invoked function) into an identifiable memory page; paragraph [0067]); and when the address of the invoked function address is found in a cache, preventing (310) execution of a payload for the invoked function (resource identifiers are translated into a representation of the instruction (function) address and include an identification of a particular processor cache resource (an address of the invoked function address is found in a cache) that is to be trapped, which includes trapping data to be sent (preventing execution of a payload); paragraphs [0138], [0211]).

As per claim 4, Sallam '018 discloses the method (300) according to claim 1, additionally Sallam '018 discloses, wherein executing (304) of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function (below-operating system security agents determine whether a given address location belonging to a particular process is associated with a user mode entries, where stack and base pointers points to the stack frames, and by walking through the base pointer through the stack, previous function calls are identified providing context for an identified operation; paragraph [0060]).

As per claim 5, Sallam '018 discloses the method (300) according to claim 1, additionally Sallam '018 discloses, wherein the monitoring (302) further comprises monitoring functions associated with memory management in the memory space by a user mode function (a below-O/S security agent is configured to intercept an attempted access of physical memory after a memory management unit/MMU has translated the virtual memory page to a physical memory address, where the operation system, O/S, is a user mode entity; paragraphs [0039], [0242]).

-***-Continued Within the Next Supplemental Box-***-

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Box V: Citations and Explanations-***-

As per claim 6, Sallam '018 discloses the method (300) according to claim 1, additionally Sallam '018 discloses, wherein the monitoring (302) further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function (below-O/S security agents operating at a level below all of the device operating systems which are user mode entities, hook various portions of an operating system to trap and evaluate low-level application operations (invoked function); abstract; paragraphs [0039], [0049], [0090]), wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function (by walking through the execution base pointer through the stack, below-O/S security agents, operating at a level below all of the device operating systems which are user mode entities, can identify previous function calls (reverse stack walk) providing context for the operations (functions) within memory; abstract; paragraphs [0039], [0049], [0060]).

As per claim 8, Sallam '018 discloses the method (300) according to claim 6, additionally Sallam '018 discloses, wherein performing (304) the one or more memory checks comprises evaluating state information associated with a cache entry for the hooked function (the security agent uses a state machine to perform trapping based on previously observed events, such as by using a hook to deny particular types of cache access; paragraphs [0090], [0193], [0207], [0214], [0269]).

As per claim 9, Sallam '018 discloses the method (300) according to claim 8, additionally Sallam '018 discloses, wherein when an address of the invoked function is found in a cache, preventing (31 0) execution of a payload for the invoked function (resource identifiers are translated into a representation of the instruction (function) address and include an identification of a particular processor cache resource (an address of the invoked function is found in a cache) that is to be trapped, which includes trapping data to be sent (preventing execution of a payload); paragraphs [0138], [0211]).

As per claim 10, Sallam '018 discloses a system (100) comprising: at least one memory (404) (a system for securing an electronic device includes a memory; paragraph [0008]); and at least one processor (402) connected with the memory (404) configured to perform operation (the system includes a processor and operating systems residing in the memory for execution by the processor; paragraph [0008]) of: monitoring (302) a memory space of a process for execution of at least one of a plurality of functions (a security agent running underneath an operating system of an electronic device monitors access by execution of key operations (plurality of functions) to system memory; paragraph [0077]); executing (304) stack walk processing upon invocation of one of the plurality of functions in the monitored memory space (by walking through the Execution Base Pointer through the stack, previous function calls are identified providing context for the operations within memory; paragraph [0060]); and performing (304), during the executing of the stack walk processing, one or more memory checks to detect suspicious behavior (by walking through the Execution Base Pointer through the stack, function calls are identified and the security agent is configured to determine whether an attempt is malicious; paragraph [0060]), wherein an alert of suspicious behavior is triggered when, during the performing of the one or more memory checks detect at least one of the following: code execution is attempted from non-executable memory (210), a base pointer is identified as being invalid (210), an invalid stack return address is identified (210), attempted execution of a return-oriented programming technique is detected (210), the base pointer is detected as being outside a current thread stack (210), and a return address is detected as being inside a virtual memory area (210) (O/S security is configured to intercept access (an alert of suspicious behavior) to memory of an electronic device such as an attempted access of pages within an address space of virtualized memory; paragraphs [0239], [0240]), wherein when an alert of suspicious behavior is triggered, the method further comprising preventing (310) execution of a payload for the invoked function (attempted access to virtualized memory address space is intercepted by O/S security, and a device security agent traps data to be sent or received (preventing execution of a payload), and scans the data payload of packets to be sent or received for evidence of malware; paragraphs [0138], [0239], [0240]).

As per claim 11, Sallam '018 discloses the system (100) according to claim 10, additionally Sallam '018 discloses, wherein the performing (304) of the one or more memory checks occur before an address of an originating caller function is reached (the trapping agent halts attempted resource access based on a triggered event, and the trapping agent adds additional context information about the attempt into the triggered event, such as the memory address from which the attempt originated (occur before an address of an originating caller function is reached); paragraph [0224]).

As per claim 12, Sallam '018 discloses the system (100) according to claim 10, additionally Sallam '018 discloses, further comprising identifying (304) an address associated with the invoked function (the security agent converts the address for a function to be trapped (invoked function) into an identifiable memory page; paragraph [0067]); and when the address of the invoked function is found in a cache, the processor (402) further executing an operation of preventing execution of a payload for the invoked function (resource identifiers are translated into a representation of the instruction (function) address and include an identification of a particular processor cache resource (an address of the invoked function address is found in a cache) that is to be trapped, which includes trapping data to be sent (preventing execution of a payload); paragraphs [0138], [0211]).

As per claim 13, Sallam '018 discloses the system (100) according to claim 10, additionally Sallam '018 discloses, wherein the executing (304) of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function (below-operating system security agents determine whether a given address location belonging to a particular process is associated with a user mode entries, where stack and base pointers points to the stack frames, and by walking through the base pointer through the stack, previous function calls are identified providing context for an identified operation; paragraph [0060]).

As per claim 14, Sallam '018 discloses the system (100) according to claim 10, additionally Sallam '018 discloses, wherein the monitoring (302) further comprises monitoring functions associated with memory management in the memory space by a user mode function (a below-O/S security agent is configured to intercept an attempted access of physical memory after a memory management unit/MMU has translated the virtual memory page to a physical memory address, where the operation system, O/S, is a user mode entity; paragraphs [0039], [0242]).

-***-Continued Within the Next Supplemental Box-***-

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Box V: Citations and Explanations-***-

As per claim 15, Sallam '018 discloses the system (100) according to claim 10, additionally Sallam '018 discloses, wherein the monitoring (302) further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function (below-O/S security agents operating at a level below all of the device operating systems which are user mode entities, hook various portions of an operating system to trap and evaluate low-level application operations (invoked function); abstract; paragraphs [0039], [0049], [0090]), and wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function (by walking through the execution base pointer through the stack, below-O/S security agents, operating at a level below all of the device operating systems which are user mode entities, can identify previous function calls (reverse stack walk) providing context for the operations (functions) within memory; abstract; paragraphs [0039], [0049], [0060]).

As per claim 17, Sallam '018 discloses the system (100) according to claim 15, additionally Sallam '018 discloses, wherein performing (304) of the memory checks comprises evaluating state information associated with a cache entry for the hooked function (the security agent uses a state machine to perform trapping based on previously observed events, such as by using a hook to deny particular types of cache access; paragraphs [0090], [0193], [0207], [0214], [0269]).

As per claim 18, Sallam '018 discloses the system (100) according to claim 17, additionally Sallam '018 discloses, wherein when an address of the invoked function is found in a cache, the processor (402) further executing an operation of preventing (310) execution of a payload for the invoked function (resource identifiers are translated into a representation of the instruction (function) address and include an identification of a particular processor cache resource (an address of the invoked function is found in a cache) that is to be trapped, which includes trapping data to be sent (preventing execution of a payload); paragraphs [0138], [0211]).

As per claim 19, Sallam '018 discloses a computer-readable storage device (404) containing instructions, that when executed on at least one processor (402), causing the processor (402) to execute a process (the system for securing an electronic device includes a processor and operating systems residing in the memory for execution by the processor; paragraph [0008]) comprising: monitoring (302) a memory space of a process for execution of at least one of a plurality of functions(a security agent running underneath an operating system of an electronic device monitors access by execution of key operations (plurality of functions) to system memory; paragraph [0077]); executing (304) stack walk processing upon invocation of one of the plurality of functions in the monitored memory space (by walking through the Execution Base Pointer through the stack, previous function calls are identified providing context for the operations within memory; paragraph [0060]); and performing (304), during the executing of the stack walk processing, at least one memory check to detect suspicious behavior (by walking through the Execution Base Pointer through the stack, function calls are identified and the security agent is configured to determine whether an attempt is malicious; paragraph [0060]), wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory (210), a base pointer is identified as being invalid (210), an invalid stack return address is identified (21 0), attempted execution of a return-oriented programming technique is detected (210), and the base pointer is detected as being outside a current thread stack (210), a return address is detected as being inside a virtual memory area (210) (O/S security is configured to intercept access (an alert of suspicious behavior) to memory of an electronic device such as an attempted access of pages within an address space of virtualized memory; paragraphs [0239], [0240]), a low level user mode function is attempted to be executed in a cache (212), wherein the cache is evaluated for an address of the invoked function, and wherein when an alert of suspicious behavior is triggered, preventing (310) execution of a payload for the invoked function (attempted access to virtualized memory address space is intercepted by O/S security, and a device security agent traps data to be sent or received (preventing execution of a payload), and scans the data payload of packets to be sent or received for evidence of malware; paragraphs [0138], [0239, [0240]).

As per claim 20, Sallam '018 discloses the computer-readable storage device (404) according to claim 19, additionally Sallam '018 discloses, wherein performing (304) of the memory check to determine if code execution is attempted from non-executable memory (security rules dictate that for a particular application, write accesses originating from programs other than the application to the portions of memory that comprise application executable code (determine if code execution is attempted from non-executable memory) indicate a malware attack; paragraph [0276]), the base pointer is identified as being invalid (by walking through the Execution Base Pointer through the stack, previous function calls can be identified, and the security agent can determine that malware may be clandestinely writing to disk outside of the functions provided by operating system; paragraphs [0049], [0060]), an invalid stack return address is identified (by walking through the Execution Base Pointer through the stack, previous function calls can be identified, and the security agent can determine that malware may be clandestinely writing to disk locations outside of the functions provided by operating system; paragraphs [0049], [0060]), execution of a return-oriented programming technique is attempted (trapping operations in firmware or at the device level can reduce the ability of malware to spoof or phish (return-oriented programming technique) elements; paragraph [0117]), the base pointer is detected as being outside a current thread stack (by walking through the Execution Base Pointer through the stack, previous function calls can be identified, and the security agent can determine that malware may be clandestinely writing to disk outside of the functions provided by operating system; paragraphs [0049], [0060]), and the return address is detected as being inside a virtual memory area (O/S security is configured to intercept access (an alert of suspicious behavior) to memory of an electronic device such as an attempted access of pages within an address space of virtualized memory; paragraphs [0239], [0240]), occurs before an address of the invoked function is reached (206) (the trapping agent halts attempted resource access based on a triggered event, and adds additional context information about the attempt into the triggered event, such as the memory address from which the attempt originated (before an address of the invoked function is reached); paragraph [0224]), and wherein the performing (304) of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing (208) (the below-O/S trapping agent halts attempted resource access based on a triggered event, and adds additional context information about the attempt into the triggered event, such as the cache memory address from which the attempt originated (before an address of the invoked function is reached), the O/S being a user mode entity; paragraphs [0039], [0207], [0224]).

-***-Continued Within the Next Supplemental Box-***-

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Box V: Citations and Explanations-***-

Claims 7 and 16 lack an inventive step under PCT Article 33(3) as being as being obvious over Sallam '018 in view of US 2012/0255013 A1 to SALLAM (hereinafter "Sallam '013"), further in view of US 2011/0145924 A1 to KOLSEK et al. (hereinafter "Kolsek"), and further in view of US 2005/0108562 A1 to KHAZAN et al. (hereinafter "Khazan").

As per claim 7, Sallam '018 discloses the method (300) according to claim 1, but does not disclose, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUseriProcess function, and an LdrLoadDll function. However, Sallam '013, discloses, wherein the plurality of functions comprises an NtAllocateVirtualMemory function (NtAllocateVirtualMemory function is provided; paragraph [0283]) and an NtProtectVirtualMemory function (NtProtectVirtualMemory function is provided; paragraph [0283]). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Sallam '018 for detecting and preventing suspicious memory operations, with the teachings of Sallam '013, in order to efficiently and conveniently provide Sallam '018 with more robust capabilities for detecting and preventing suspicious memory operations. Sallam '018 and Sallam '013 do not disclose wherein the plurality of functions comprises an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUseriProcess function, and an LdrLoadDll function. However, Kolsek discloses, wherein the plurality of functions comprises an NtCreateProcess function (NtCreateProcess function is provided; paragraph [0056]), an NtCreateUseriProcess function (NtCreateProcess and CreateProcessAsUserA (NtCreateUseriProcess) functions are provided; paragraphs [0056], [0058], [0065]), and an LdrLoadDll function (LdrLoadDll function is provided; paragraph [0052]). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Sallam '018 and Sallam '013 for detecting and preventing suspicious memory operations, with the teachings of Kolsek, in order to efficiently and conveniently provide Sallam '018 and Sallam '013 with more robust capabilities for detecting and preventing suspicious memory operations. Sallam '018, Sallam '013, and Kolsek do not disclose wherein the plurality of functions comprises an NtCreateProcessEX function. However, Khazan discloses, wherein the plurality of functions comprises an NtCreateProcessEX function (CreateProcessEX function is provided; paragraph [0076]). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Sallam '018, Sallam '013, and Kolsek for detecting and preventing suspicious memory operations, with the teachings of Khazan, in order to efficiently and conveniently provide Sallam '018, Sallam '013, and Kolsek with more robust capabilities for detecting and preventing suspicious memory operations.

As per claim 16, Sallam '018 discloses the system (100) according to claim 10, but does not disclose, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUseriProcess function, and an LdrLoadDll function. However, Sallam '013, discloses, wherein the plurality of functions comprises an NtAllocateVirtualMemory function (NtAllocateVirtualMemory function is provided; paragraph [0283]) and an NtProtectVirtualMemory function (NtProtectVirtualMemory function is provided; paragraph [0283]). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Sallam '018 for detecting and preventing suspicious memory operations, with the teachings of Sallam '013, in order to efficiently and conveniently provide Sallam '018 with more robust capabilities for detecting and preventing suspicious memory operations. Sallam '018 and Sallam '013 doe not disclose wherein the plurality of functions comprises an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUseriProcess function, and an LdrLoadDll function. However, Kolsek discloses, wherein the plurality of functions comprises an NtCreateProcess function (NtCreateProcess function is provided; paragraph [0056]), an NtCreateUseriProcess function (NtCreateProcess and CreateProcessAsUserA (NtCreateUseriProcess) functions are provided; paragraphs [0056], [0058], [0065]), and an LdrLoadDll function (LdrLoadDll function is provided; paragraph [0052]). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Sallam '018 and Sallam '013 for detecting and preventing suspicious memory operations, with the teachings of Kolsek, in order to efficiently and conveniently provide Sallam '018 and Sallam '013 with more robust capabilities for detecting and preventing suspicious memory operations. Sallam '018, Sallam '013, and Kolsek do not disclose wherein the plurality of functions comprises an NtCreateProcessEX function. However, Khazan discloses, wherein the plurality of functions comprises an NtCreateProcessEX function (CreateProcessEX function is provided; paragraph [0076]). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Sallam '018, Sallam '013, and Kolsek for detecting and preventing suspicious memory operations, with the teachings of Khazan, in order to efficiently and conveniently provide Sallam '018, Sallam '013, and Kolsek with more robust capabilities for detecting and preventing suspicious memory operations.

Claims 1-20 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

PCT Recordation of Search History

Case/PCT Application Number: PCT/US15/13111

CLIN Number/Technical Field of PCT Application: 4

Date(s) During Which the Search was Conducted: 2 April 2015 - 4 April 2015

Date of Completion of Recordation of Search History Form: 4 April 2015

Research Analyst Initials: OVM

Search Approval Official (SAO) Initials: HKP

Field of Search/Classification Information:

IPC(8) Classification(s): G06F 21/50, 21/52, 21/54, 21/55, 21/12, 21/14; H04L 29/06 (2015.01)

CPC Classification(s): G06F 21/50, 21/52, 21/54, 21/552, 21/577; H04L 63/1441, 63/1416, 63/1466

Database(s) Searched (Patent and Non-Patent Literature (NPL), Including Sub-Databases and Files Searched) and Search Terms Used:

PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, INPADOC); ProQuest; IEEE/IEEEXplore; Google/Google Scholar;

track*, monitor*, detect*, check*, memor*, function*, call*, stack*, walk*, intrusi*, suspicious*, exploit*, malicious*, invalid*, prevent*, payload*

Database Search String Recordation, Including Dates of Searches):
Patent Database Search Strategy/Results:

Patseer (4 April 2015):

ID	Search String	Deduped	Records	Created Date
L38	TACD :((track* OR monitor* OR check*) w3 memor*) AND stack* AND function* AND call* AND ((intrusi* OR suspicious* OR malicious* OR exploit*) w3 (prevent* OR detect*)) AND walk* AND address* AND invalid	-	136	1-Apr-15
L37	TACD :((track* OR monitor* OR check*) w3 memor*) AND stack* AND function* AND call* AND ((intrusi* OR suspicious* OR malicious* OR exploit*) w3 (prevent* OR detect*)) AND walk* AND address*	-	287	1-Apr-15
L36	TACD :((track* OR monitor* OR check*) w3 memor*) AND stack* AND function* AND call* AND ((intrusi* OR suspicious* OR malicious* OR exploit*) w3 detect*) AND walk* AND prevent* AND address*	-	214	1-Apr-15
L35	TACD :((track* OR monitor* OR check*) w3 memor*) AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*) AND walk* AND prevent* AND address* AND payload*	-	295	1-Apr-15
L34	TACD :((track* OR monitor* OR check*) w3 memor*) AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*) AND walk* AND prevent* AND address*	-	989	1-Apr-15
L33	TACD :((track* OR monitor* OR check*) w3 memor*) AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*) AND walk* AND prevent*	-	1000	1-Apr-15
L32	TACD :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*) AND walk* AND prevent*	-	5912	1-Apr-15
L31	TACD :(track* OR monitor* OR detect* OR check*) AND memor* AND stack*	-	6985	1-Apr-15

	AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*) AND walk*			
L30	TAC :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*) AND walk*	-	17	1-Apr-15
L29	TA :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*) AND walk*	-	0	1-Apr-15
L28	TACD :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*)	-	56951	1-Apr-15
L27	TAC :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*)	-	200	1-Apr-15
L26	TA :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious* OR exploit*)	-	11	1-Apr-15
L25	TAC :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call*	-	1885	1-Apr-15
L24	TA :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function* AND call*	-	70	1-Apr-15
L23	TAC :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function*	-	6731	1-Apr-15
L22	TA :(track* OR monitor* OR detect* OR check*) AND memor* AND stack* AND function*	-	275	1-Apr-15
L21	TA :(memor* AND stack* AND function*)	-	1896	1-Apr-15
L20	TACD :(memor* AND stack* AND function*) CPC :("H04L63/1466")	-	289	1-Apr-15
L19	TACD :(memor* AND stack* AND function*)	-	925	1-Apr-15

	CPC :("H04L63/1416")			
L18	TACD :(memor* AND stack* AND function*) CPC :("H04L63/1441")	-	647	1-Apr-15
L17	TACD :(memor* AND stack* AND function*) CPC :("G06F21/577")	-	421	1-Apr-15
L16	TACD :(memor* AND stack* AND function*) CPC :("G06F21/552")	-	432	1-Apr-15
L15	TACD :(memor* AND stack* AND function*) CPC :("G06F21/54")	-	430	1-Apr-15
L14	TACD :(memor* AND stack* AND function*) CPC :("G06F21/52")	-	821	1-Apr-15
L13	TACD :(memor* AND stack* AND function*) CPC :("G06F21/50 ")	-	164	1-Apr-15
L12	TACD :(memor* AND stack* AND function*) IC :("H04L29/06 ")	-	27749	1-Apr-15
L11	TACD :(memor* AND stack* AND function*) IC :("G06F21/14")	-	116	1-Apr-15
L10	TACD :(memor* AND stack* AND function*) IC :("G06F21/12")	-	211	1-Apr-15
L9	TACD :(memor* AND stack* AND function*) IC :("G06F21/55")	-	265	1-Apr-15
L8	TACD :(memor* AND stack* AND function*) IC :("G06F21/54")	-	123	1-Apr-15
L7	TACD :(memor* AND stack* AND function*) IC :("G06F21/52")	-	226	1-Apr-15
L6	TACD :(memor* AND stack*) IC :("G06F21/50")	-	102	1-Apr-15
L5	TACD :(memor* AND stack* AND function*) IC :("G06F21/50")	-	101	1-Apr-15
L4	ASNN :(WEBROOT*) INV :(BIZZARRI OR VOLTATTORNI OR MAYR)	-	2	1-Apr-15
L3	ASNN :(WEBROOT*)	-	4	1-Apr-

	INV :(GIULIANI)			15
L2	ASNN :(WEBROOT*) INV :(GIULIANI OR BIZZARRI OR VOLTATTORNI OR MAYR)	-	4	1-Apr-15
L1	ASNN :(WEBROOT*)	-	114	1-Apr-15

Non-Patent Literature (NPL) Search Strategy/Results:

IEEE/IEEEXplore (Search Date: 4 April 2015):

- (track* OR monitor* OR detect* OR check*) AND (memor*) AND stack* AND function* AND call*
- (track* OR monitor* OR detect* OR check*) AND (memor*) AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious*)
- (track* OR monitor* OR detect* OR check*) AND (memor*) AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious*) AND walk*

Google/Google Scholar (Search Date: 3 April 2015):

- memory monitoring call stack walk
- tracking memory intrusion call
- detect memory call exploits

IP.com (Search Date: 2 April 2015):

- (track* OR monitor* OR detect* OR check*) AND (memor*) AND stack* AND function* AND call*
- (track* OR monitor* OR detect* OR check*) AND (memor*) AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious*)
- (track* OR monitor* OR detect* OR check*) AND (memor*) AND stack* AND function* AND call* AND (intrusi* OR suspicious* OR malicious*) AND walk*

Electronic Acknowledgement Receipt

EFS ID:	22358462
Application Number:	14606604
International Application Number:	
Confirmation Number:	7326
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0117USU1
Receipt Date:	15-MAY-2015
Filing Date:	27-JAN-2015
Time Stamp:	13:07:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	2015_05_15_IDS_SB08_04584_0117USU1.PDF	612227 8b34379fa472e05faf474dadd2c40b164a0221fb	no	4

Warnings:

Information:

2	Non Patent Literature	ISR_WO_PCTUS15_13111_04_17_15_15pgs.PDF	754030 632ef35f5e8467767a2f48257687a55be67f4916	no	15
Warnings:					
Information:					
			Total Files Size (in bytes):	1366257	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
14/606,604

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/606,604	01/27/2015	2431	730	04584.0117USU1	20	3

CONFIRMATION NO. 7326

23552
MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

FILING RECEIPT

OC000000073275727

Date Mailed: 02/09/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Marco Giuliani, Bastia Umbra (PG), ITALY;
Marco Bizzarri, Sassoferrato (AN), ITALY;
Benedetto Voltattorni, San Benedetto del Tronto (AP), ITALY;
Johannes Mayr, Linz, AUSTRIA;

Applicant(s)

WEBROOT INC., Broomfield, CO

Assignment For Published Patent Application

WEBROOT INC., Broomfield, CO

Power of Attorney: The patent practitioners associated with Customer Number 23552

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/931,772 01/27/2014

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 02/06/2015
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/606,604**

Trend Micro, Inc.
EX1006-177

Projected Publication Date: 07/30/2015

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

Trend Micro, Inc.
EX1006-178

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Trend Micro, Inc.
EX1006-179

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	Filed herewith
Filing Date	Filed herewith
First Named Inventor	Marco Giuliani
Title	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
Art Unit	Not assigned
Examiner Name	Not assigned
Attorney Docket Number	04584.0117USU1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Jason E. Becker/	Date (Optional)	1/27/2015
Name	Jason E. Becker	Registration Number	66632
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 23552

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

WEBROOT INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	May 12, 2014
Name	Ryan Howe		
Title	Associate General Counsel		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Filer:	Jason Evan Becker/Jacquelyn Slate
Attorney Docket Number:	04584.0117USU1

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**730**

Electronic Acknowledgement Receipt

EFS ID:	21322645
Application Number:	14606604
International Application Number:	
Confirmation Number:	7326
Title of Invention:	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS
First Named Inventor/Applicant Name:	Marco Giuliani
Customer Number:	23552
Filer:	Jason Evan Becker/Jacquelyn Slate
Filer Authorized By:	Jason Evan Becker
Attorney Docket Number:	04584.0117USU1
Receipt Date:	27-JAN-2015
Filing Date:	
Time Stamp:	16:18:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$730
RAM confirmation Number	2398
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	2015_01_27_ADS_04584_0117USU1.PDF	1561357 f843ac50c7bdfd160166decdbef69e95cacb210a	no	8
Warnings:					
Information:					
2		2015_01_27_SpecificationAsFiled_04584_0117USU1.PDF	180305 98886fd657f097c8f1d44f71e53bf8cec5041d32	yes	26

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	20
Claims	21	25
Abstract	26	26

Warnings:					
Information:					
3	Drawings-only black and white line drawings	2015_01_27_FiguresAsFiled_04584_0117USU1.PDF	149225 b1202c0406ca4d3b9527f289bfd30aedf228086f	no	4
Warnings:					
Information:					
4	Oath or Declaration filed	2015_01_27_Dec_Executed_04584_0117USU1.PDF	5381992 0af0506e98e1e6403ab7da44effd223a118c7251	no	8
Warnings:					
Information:					
5	Power of Attorney	2015_01_27_POA_04584_0117USU1.PDF	283006 d392cb31c73b405274a0163ee24e8e6b018613ea	no	2
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

6	Fee Worksheet (SB06)	fee-info.pdf	35505 40ecfa5421ad8c56e098f4ab2251ada15519578b	no	2

Warnings:

Information:

Total Files Size (in bytes):	7591390

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0117USU1
	Application Number	
Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Marco		Giuliani	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Bastia Umbra (PG)	Country of Residence i	IT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent		
City	Broomfield	**State/Province**	CO
Postal Code	80021	**Country** i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Marco		Bizzarri	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Sassoferrato (AN)	Country of Residence i	IT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent		
City	Broomfield	**State/Province**	CO
Postal Code	80021	**Country** i	US

Inventor 3 Remove

Legal Name

Trend Micro, Inc.
EX1006-187

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0117USU1
	Application Number	
Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Benedetto		Voltattorni	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	San Benedetto del Tronto (AP)	Country of Residence i	IT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent		
City	Broomfield	**State/Province**	CO
Postal Code	80021	**Country** i	US

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Johannes		Mayr	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Linz	Country of Residence i	AT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent		
City	Broomfield	**State/Province**	CO
Postal Code	80021	**Country** i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	23552	
Email Address	DOCKMPLS@merchantgould.com	Add Email Remove Email

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0117USU1
	Application Number	
Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS	

Application Information:

Title of the Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS		
Attorney Docket Number	04584.0117USU1	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	**Suggested Figure for Publication (if any)**	3

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	◯ US Patent Practitioner	◯ Limited Recognition (37 CFR 11.9)
Customer Number	23552		

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0117USU1
	Application Number	
Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Claims benefit of provisional	61/931772	2014-01-27

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Trend Micro, Inc.
EX1006-190

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0117USU1
	Application Number	
Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS	

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Webroot Inc.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0117USU1
	Application Number	
Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS	

Mailing Address Information:			
Address 1	385 Interlocken Crescent		
Address 2			
City	Broomfield	**State/Province**	CO
Country i	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	Webroot Inc.

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	385 Interlocken Crescent		
Address 2			
City	Broomfield	**State/Province**	CO
Country i	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Jason E. Becker/	Date (YYYY-MM-DD)	2015-01-27

Trend Micro, Inc.
EX1006-192

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0117USU1
	Application Number	
Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS	

First Name	Jason E.	Last Name	Becker	Registration Number	66632
Additional Signature may be generated within this form by selecting the Add button.				Add	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

Priority

[0001] This application claims the benefit of U.S. Provisional Application No. 61/931,772, filed on January 27, 2014, which is hereby incorporated by reference in its entirety.

Background

[0002] An exploit is a piece of code, software, data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or any other electronic component. Exploits are usually intended for malicious purposes and pose threats that can compromise a computing system or device, for example, by hijacking normal code flow execution of a process towards a zone of memory where exploit code currently stands. For instance, exploit code may launch a new process or manipulate an existing process to perform malicious execution. Prevention of software exploits from executing code is a paramount security concern for system users and administrators. It is with respect to this general environment that aspects of the present technology disclosed herein have been contemplated.

Summary

[0003] Aspects of the present disclosure relate to anti-exploit examples. In non-limiting examples, anti-exploit systems and methods described herein monitor a memory space of a process for execution of functions. Stack walk processing is executed upon invocation of one of the functions in the monitored memory space. During execution of the stack walk processing, at least one memory check is performed to detect suspicious behavior. An alert of suspicious behavior is triggered when the performing of the memory check detects at least one of: code execution attempted from non-executable memory, identification of an invalid base pointer, identification of an invalid stack return address, attempted execution of a return-oriented programming technique, the base pointer is

outside a current thread stack, and a return address is detected as being inside a virtual memory area. If an alert of suspicious behavior is triggered, execution of a payload is prevented for the invoked function.

[0004] In other non-limiting examples, the anti-exploit examples described herein monitor a memory space of a process for execution of functions. Stack walk processing is executed upon invocation of one of the functions in the monitored memory space. During execution of the stack walk processing, at least one memory check is performed to detect suspicious behavior. An alert of suspicious behavior is triggered when the performing of the memory check detects at least one of: code execution attempted from non-executable memory, identification of an invalid base pointer, identification of an invalid stack return address, attempted execution of a return-oriented programming technique, the base pointer is outside a current thread stack, a return address is detected as being inside a virtual memory area, and a low level user mode function is attempted to be executed in a cache, where the cache is evaluated for identification of an address of the invoked function. One of skill in the art will appreciate that the embodiments disclosed herein can be employed to detect other types of suspicious behavior. If an alert of suspicious behavior is triggered, action is taken to prevent execution of a payload for the invoked function.

[0005] This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

Brief Description of the Drawings

[0006] Non-limiting and non-exhaustive examples are described with reference to the following figures. As a note, the same number represents the same element or same type of element in all drawings.

[0007] Figure 1 illustrates an exemplary system 100 showing interaction of components for implementation of exemplary anti-exploit examples described herein.

Trend Micro, Inc.
EX1006-196

[0008] Figure 2 illustrates an exemplary chart 200 of one or more memory checks performed by the anti-exploit examples described herein.

[0009] Figure 3 illustrates an exemplary method 300 for implementation of anti-exploit systems and methods described herein.

[0010] Figure 4 illustrates one example of a suitable operating environment 400 in which one or more of the present examples may be implemented.

Detailed Description

[0011] Non-limiting examples of the present disclosure provide anti-exploit examples that prevent exploit code from being executed. Examples describe monitoring of memory process control flow in order to detect potential suspicious behavior and performing at least one check to evaluate how memory is being allocated before setting/marking an area of memory space as suspicious. By analyzing characteristics of memory space where a function is called from, the anti-exploit examples are able to effectively and accurately determine whether an exploit is attempting to execute its own code or if intended execution of application code is normal system behavior.

[0012] A number of technical advantages are achieved based on the present disclosure including but not limited to: enhanced security protection, improved detection of potential security exploits, reduction in error rate in identification and marking of suspicious behavior (e.g., false positives), and improved usability and interaction with users who are not required to continuously monitor for security exploits, among other examples.

[0013] Figure 1 illustrates an exemplary system 100 showing interaction of components for implementation of exemplary anti-exploit technology described herein. Exemplary system 100 presented is a combination of interdependent components that interact to form an integrated whole for execution of exploit detection and prevention operations. Components of the systems may be hardware components or software implemented on and/or executed by hardware components of the systems. In examples, system 100 may include any of hardware components (e.g., used to execute/run operating system (OS)),

Trend Micro, Inc.
EX1006-197

software components (e.g., applications, application programming interfaces, modules, virtual machines, runtime libraries, etc.) running on hardware. In one example, an exemplary system 100 may provide an environment for software components to run, obey constraints set for operating, and makes use of resources or facilities of the system 100, where components may be software (e.g., application, program, module, etc.) running on one or more processing devices. For instance, an anti-exploit mechanism (e.g., application, instructions, modules, etc.) may be run on a processing device such as a computer, mobile device (e.g., smartphone/phone, tablet) and any other electronic devices, where components of the system may be executed on the processing device. In other examples, the components of systems disclosed herein may be spread across multiple devices. For instance, input may be entered on a client device (e.g., mobile phone) and information may be processed or accessed from other devices in a network such as one or more server devices used to implement an anti-exploit mechanism or protocol.

[0014] As one example, the system 100 comprises an anti-exploit component 102, a cache component 104, and a memory component 106, each having one or more additional components. The scale of systems such as system 100 may vary and include more or less components than those described in Figure 1. In some examples, interfacing between components of the system 100 may occur remotely, for example where anti-exploit technology is implemented remotely to monitor and control process flow for detection of suspicious behavior (e.g., exploit) and prevention of execution of code of the suspicious behavior.

[0015] An anti-exploit component 102 implements anti-exploit examples described herein to detect suspicious behavior and prevent exploit code of software exploits from being executed. An exploit is a piece of code, software, data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior. Example types of exploits include malware such as computer viruses, worms, trojan horses, spyware and adware, among other examples. As an example, the anti-exploit examples described herein prevent exploit code of a process from executing another process or loading a module into the process memory. The anti-

Trend Micro, Inc.
EX1006-198

exploit examples implemented by the anti-exploit component 102 are able to be configured to detect and prevent software exploits that attempt to execute another process or load a module into process memory, for instance, a process where shellcode is able to be injected and executed.

[0016] An action of calling a system process (e.g., function of an application or application programming interface (API)) from a low level perspective, involves the presence of a particular set of assembly instruction, such as a CALL, inside the process memory. A low level operation or instruction provides minimal abstraction from a computer's instruction set architecture, for example either machine code or assembly language. The word "low" refers to the small or nonexistent amount of abstraction between the programming language and machine language. Low-level languages can be converted to machine code without using a compiler or interpreter, and the resulting code runs directly on the processor. Once the CALL instruction is reached, the code flow of the program starts to follow a chain of functions which will lead to the lowest level user mode function, before transitioning to Kernel Mode. In Kernel mode, the executing code has complete and unrestricted access to the underlying hardware. It can execute any CPU instruction and reference any memory address. Kernel mode is generally reserved for the lowest-level, most trusted functions of the operating system. In user mode, the executing code has no ability to directly access hardware or reference memory. Code running in user mode must delegate to system APIs to access hardware or memory. Most of the code running on a processing device such as a computer will execute in user mode. Thus, an instruction from user mode involves system call instructions (e.g., triggering operating system dependent software interrupt or control transfer instructions such as a sysenter assembly instruction) to execute a kernel function.

[0017] Generally, a non-malicious call starts from a range of pages in a zone of memory containing application or system module execution code. This zone of memory contains data (e.g., pages) used to store a module (e.g., executable file (.exe) or dynamic-link library (DLL)) assembly code. The zone of memory may share physical storage with other processes. As an example, the zone of memory may be marked as MEM_IMAGE. The anti-exploit described herein detect functions called from user mode, for example,

Trend Micro, Inc.
EX1006-199

that attempt to allocate new pages of memory, reallocate system memory or modify the type of a memory page. In examples, an exploit may be initiated from another zone of memory (e.g., outside of the MEM_IMAGE zone/region such as a non MEM_IMAGE region). In another example, an exploit may attempt alter instruction sequences within a system memory region such as MEM_IMAGE, for example, by return-oriented programming (ROP). The anti-exploit component 102 monitors for, detects, and takes action to prevent such suspicious behavior.

[0018] In order to reach a goal of starting a new process, an exploit has to execute a complete execution stack starting from the shellcode and running down through to a lowest level user function (e.g., instruction that includes machine or assembly instruction). Shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability. An exploit will commonly inject shellcode into the target process before or at the same time as it exploits a vulnerability to gain control over a program counter. The program counter is adjusted to point to the shellcode, after which the shellcode (including the malicious payload) is executed.

[0019] The anti-exploit component 102 executes a function hooking technique to hook to the lowest level user mode function and intercept system routines of a called API. A hooking technique covers a range of techniques used to alter or augment the behavior of an operating system, of applications, or of other software components by intercepting function calls or messages or events passed between software components. A hook is code that handles such intercepted function calls, events or messages.

[0020] The anti-exploit component 102 loads a component such as a custom module into the memory space of each monitored process. This component intercepts monitored operating system applications or APIs and evaluates a record (e.g., stack frame) of a call stack. A stack frame is a frame of data that gets pushed onto a stack that stores information about the active subroutines of a computer program. As an example, a stack frame may represent a function call and its argument data.

[0021] When unidentified code tries to allocate/mark a new executable page of memory which is not related to any valid process module, the custom component monitors these

Trend Micro, Inc.
EX1006-200

newly allocated memory regions and prevents any attempted execution of monitored functions. Functions monitored comprise processes that attempt execution of another process or loading of a module into a process memory, for example, function such as NtCreateProcess, NtCreateProcessEX, NtCreateUserProcess, LdrLoadDll, among other examples monitored functions. The present application is not limited to functions of a specific operating system. One skilled in the art will appreciate that the embodiments disclosed herein can be employed to cover functions that attempt execution of another process or loading of a module into a process memory, implementable by/in other operating systems. The anti-exploit examples of the anti-exploit component 102 are configurable to be programmed to monitor any type of function of an application/API. A list of monitored functions may be maintained by the anti-exploit component 102. Examples of functions monitored by the anti-exploit technology include but are not limited to: NtAllocateVirtualMemory, NtProtectVirtualMemory, NtCreateProcess, NtCreateProcessEX, NtCreateUserProcess, LdrLoadDll, among other examples. Again, one skilled in the art will appreciate that the embodiments disclosed herein can be employed to monitor any functions that attempt execution of another process or loading of a module into a process memory, implementable by/in other operating systems. The list of monitored functions may change perpetually and can be updated (e.g., by an administrator or software update) at any time to improve the robustness of the functions monitored and improve security against software exploits. The function hooking technique of the anti-exploit component 102 intercepts the system routines of the called process.

[0022] A hooked function (including but not limited to NtCreateProcess, NtCreateProcessEX, NtCreateUserProcess, LdrLoadDll) is monitored/evaluated through execution of stack walk processing. The anti-exploit component 102 executes stack walk processing that walks up a call stack for the process (function) until an address of the first function of a called function is reached. As an example, for stack walk processing, when one of the functions listed before is invoked, the first step is to get the value of the call frame pointer for being able to walk the call stack frame. The call frame pointer contains the address of the stack frame for the called function. In the examples disclosed herein, the anti-exploit technology may go back through the stack_entry chain until the initial

caller's stack frame is reached (e.g., back-walk the stack frame starting from the lowest level user mode function to an address where the call sequence started for the hooked function). Once reached, an address from where the call sequence has started for the hooked function is located and characteristics of that particular memory region are retrieved and analyzed (e.g., evaluating state information of the particular memory region). In the stack walk processing, an address of a base pointer of the stack and an address of a stack pointer are identified for a stack frame associated with the called function. As an example of a base pointer, a precFp may be identified. A precFp is a pointer to the previous STACK_ENTRY structure of the called function. The retAddr is the address where the control flow must continue after the called function has completed. Each time a CALL is executed, a new stack frame is created and the return address is set with the value of the instruction following CALL opcode (e.g., portion of machine language instruction that specifies an operation to be performed).

[0023] During the stack walk processing of the stack frame, a first call address of a call sequence is one that is present in the last valid stack entry. A list of conditions may be evaluated against each stack entry found during the stack walk. As examples, a stack frame of a called function may be required to satisfy conditions such as:

- both, precFp and retAddr, must be valid accessible addresses (verified via system APIs, for example VirtualQuery() and TestVirtualMemoryAccess()); and

- if these addresses are valid, then the previous 10 bytes before the retAddr address are parsed, searching for a CALL assembly instruction of the hooked function. Every time a CALL instruction is executed, a new stack frame is created and the return address is set with the value of the address of the instruction following the CALL op-code.

[0024] In a case where conditions, such as the above identified conditions, are satisfied, the stack walk processing may proceed with evaluating a memory region associated with a called function. For example, stack walk processing may include performing one or more memory checks from the lowest level user function of the hooked function down through the address of the originating caller function (e.g., the hooked function). Once

the address is located from where the call sequence has started, characteristics of that particular memory region are retrieved and analyzed. In analyzing the characteristics of the memory region, the memory region data (e.g., memory pages) maintained in a cache by the anti-exploit examples disclosed herein are evaluated during performance of a memory check. The stack walk processing executed by the anti-exploit component 102 performs a memory check or checks on a frame of call stack pertaining to the called process (including one or more functions) attempting to detect and identify suspicious behavior that may pertain to a software exploit. Examples of memory checks performed are provided in a later description of Figure 2. Unlike other exploit prevention technologies that try to prevent that an exploit starts its own shellcode, the anti-exploit examples implemented by the anti-exploit component 102 prevent that the shellcode performs an ultimate execution of a malicious payload, whether the malicious payload is loading another module or executing another process.

[0025] The anti-exploit component 102 interfaces with a cache component 104 as shown in system 100 of Figure 1. The cache component 104 is a structure (hardware or software) that stores data related to a memory region for a monitored process. Memory used for a cache is allocated by the anti-exploit technology, for example by the anti-exploit component 102. The cache component 104 maintains a cache for a monitored process. A cache is a specific memory region allocated in each monitored process where information about monitored memory pages is tracked. In an example, the cache component 104 interface with the anti-exploit component 102 during hooking of a monitored function to store state information about pages of memory associated with the called function when the permission is changed, for example, changing the permission to "execute." State information tracked by the cache component 104 comprises information about the allocation of memory pages for a monitored process and the initial permissions and type of the memory pages as well as any later changes of permissions for each memory page. In at least one variation of system 100, the cache component 104 may be included in the anti-exploit component 102. While Figure 1 illustrates the cache component 104 as a separate component from the anti-exploit component 102 for ease of explanation, the anti-exploit technology implemented may be a collection of operations that include the ability to cache data.

Trend Micro, Inc.
EX1006-203

[0026] During execution of the stack walk processing, the cache component 104 tracks and evaluates the state information about pages of memory relate to a monitored process. The hooked function is triggered and a back-walk of the stack frame is initiated, where the back-walk walks up the call stack from the lowest level user mode function (hooked function) until the first function of the chain is reached. The anti-exploit component 102 interfaces with the cache component 104 to evaluate the tracked memory information for a monitored process, for example while a memory check is being performed during the stack walk processing. The tracked memory information in the cache component 104 is evaluated before the anti-exploit technology allows code of the process to access memory space (e.g., system memory) of the memory component 106. Memory checks performed pertaining to tracked data in the cache may trigger an alert of suspicious behavior, for example, where the anti-exploit component 102 identifies what it believes to be shellcode and prevents execution of a malicious payload of the shellcode.

[0027] The cache component 104 is implementable as a linked list of nodes. Each node entry stores specific data (including the nature of the potential attack) about a memory region that is monitored. A new node may be added any time system service routines are invoked related to a memory space. Examples of system services routines associated with memory include functions similar to NtAllocateVirtualMemory or NtProtectVirtualMemory.

[0028] As an example, a function that may be monitored is a function associated with creation or allocation of at least one region in a memory space (e.g., virtual memory space). For instance, NtAllocateVirtualMemory is a routine invoked in order to reserve, commit, or both, a region of pages within the user-mode virtual address space of the process. As an example, a new node is created if the memory is allocated as PAGE_EXECUTE_READWRITE in a non MEM_IMAGE region or in case a suspicious behavior matching logic rules was found during the stack walk.

[0029] As another example, a function associated with protection or change to protection in at least one region of a memory space (e.g., virtual memory space) may be monitored. For instance, NtProtectVirtualMemory is a routine invoked in order to change the

Trend Micro, Inc.
EX1006-204

protection on a region of committed pages of the virtual address space of the process. As an example, a new node is created if the memory protection of a non MEM_IMAGE region is changed to PAGE_EXECUTE_READWRITE and the prior protection/permission assigned to the page was non-executable or in case a suspicious behavior matching logic rules was found during the stack walk.

[0030] When a memory check performed during the stack walk processing does not trigger an alert of suspicious behavior, the anti-exploit component 102 enables a complete called function to access the a system kernel via the memory component 106. The memory component 106 is one or more structures (hardware or software) of system memory. In a case where a memory check performed during the stack walk processing triggers an alert of suspicious behavior (e.g., a potential security exploit), the anti-exploit component 102 prevents the execution of the payload of the called function, thus preventing access to the memory component 106.

[0031] Figure 2 illustrates an exemplary chart 200 of memory checks performed by the anti-exploit examples described herein. Chart 200 identifies exemplary memory checks performed during stack walk processing. As referenced above, a stack-walk is executed in reverse order from a system call-up to an initiating caller address, which could be shellcode. By performing the memory checks during the stack walk processing (e.g., back-walk of the stack frame), shellcode is able to be prevented from performing execution of a malicious payload.

[0032] In chart 200, column 202 identifies a timing associated with performance of exemplary memory checks and comprises rows 206 and 208. Row 206 identifies a timing of performing memory checks before an address is reached for an originating caller function. Memory checks performed during the stack walk processing at a timing before an address is reached for an originating caller function (row 206), include the memory checks identified in block 210. Row 208 identifies a timing of performing memory checks once an address is reached for an originating caller function. Memory checks performed during the stack walk processing once an address is reached for an originating caller function (row 208), include the memory checks identified in block 212.

Trend Micro, Inc.
EX1006-205

[0033] Memory checks (identified in block 210) are made continuously during the stack walk processing until the address of an originating caller function (e.g., hooked function) is reached. At least one additional memory check (block 212) is made if the address of the originating caller function is reached. An example of an originating caller function is the hooked and monitored function that is associated with the stack frame being evaluated.

[0034] Memory checks (column 204) performed at a timing (column 202) before an address for an originating caller function is reached (as indicated in row 206) are shown in block 210. Block 210 includes, but is not limited to, the following memory checks:

- Is code execution attempted from non-executable memory;
- Is a base pointer of a stack frame identified as being invalid;
- Is invalid stack return address identified for a stack frame;
- Is attempted execution of a return-oriented programming technique detected;
- Is the base pointer of a stack frame detected as being outside a current thread stack, and
- Is a return address detected as being inside a virtual memory area.

[0035] One of skill in the art will appreciate that a subset of these checks or other checks not listed may be performed without departing from the spirit of this disclosure.

[0036] For detection of code execution from non-executable memory as shown in block 210, the systems and methods disclosed herein determine whether a process is being loaded from a memory address of the memory space that is marked as non-executable or if a return address found in the stack walk chain falls in a non-executable memory. As an example, the anti-exploit examples may look for flags indicating that a process is associated with non-executable memory of the memory space. For instance, flags indicating functions similar to PAGE_EXECUTE, PAGE_EXECUTE_READ, PAGE_EXECUTE_READWRITE or PAGE_EXECUTE_WRITECOPY, can trigger an alert of suspicious behavior.

[0037] For detection of an invalid base pointer (e.g., base stack pointer) as shown in block 210, anti-exploit systems and methods evaluate whether a memory address associated with a base pointer of a stack frame fails into a memory address that is not accessible or not allocated. For example, if a base pointer for a current stack frame (e.g., current EBP) during the stack walk falls into a memory address that is not accessible or not allocated, an alert of suspicious behavior is triggered. In a case where an invalid base pointer is found inside a virtual memory management API, the address will be saved in the local cache and further evaluated using an additional memory check such as whether execution of an originating caller function is attempted in the cache once the address for the originating caller function is reached in the stack walk processing. If instead the behavior is found from an API process such as or similar to loadImage/createprocess, an alert of suspicious behavior will be triggered immediately.

[0038] An alert of suspicious behavior is triggered when an invalid stack return address is detected as shown in block 210. Anti-exploit systems and methods evaluate if the current stack pointer during the stack walk falls into a memory address that is not accessible. If so, an alert is triggered. In the case an invalid stack return address is found inside a virtual memory management API, the address will be saved in the local cache. If instead the behavior is found from an API process such as or similar to loadImage/createprocess, an alert of suspicious behavior will be triggered immediately.

[0039] If the current return address during the stack walk is a ROP gadget as shown in block 210, anti-exploit systems and methods trigger an alert of suspicious behavior. A ROP gadget is a security exploit that executes carefully chosen machine instruction sequences. Some exploit scenarios describe previously relate to injecting code into an API and getting the injected code executed. In evaluating a ROP gadget, this memory check evaluates whether API code (without injecting code) is to be executed out of sequence, for example, where a ROP gadget may force API code to jump to another place of code in an order intended to exploit the API code. In a case where a ROP gadget is found inside a virtual memory management API, the address will be saved in the local cache and further evaluated using an additional memory check such as whether execution of an originating caller function is attempted in the cache once the address for the

Trend Micro, Inc.
EX1006-207

originating caller function is reached in the stack walk processing. If instead the behavior is found from an API process such as or similar to loadImage/createprocess, an alert of suspicious behavior will be triggered immediately.

[0040] In some cases, a base pointer may be valid and accessible outside a current thread stack for a stack frame being evaluated as shown in block 210. In examples, when a base pointer is outside a current thread stack an alert for suspicious behavior is triggered. In the case where a base pointer is outside a current thread stack but inside a virtual memory management API, the address will be saved in the local cache and further evaluated using an additional memory check such as determining whether execution of an originating caller function is attempted in the cache once the address for the originating caller function is reached in the stack walk processing. If instead the behavior is found from an API process such as or similar to loadImage/createprocess, an alert of suspicious behavior will be triggered immediately.

[0041] Another memory check shown in block 210 is performed to evaluate whether a return address is detected as being inside a virtual memory area that is going to be marked or allocated as executable. If the current return address during the stack walk chain falls into the memory area which is going to be allocated/marked as executable an alert will be triggered immediately.

[0042] Once the address of the originating caller function is reached in the stack walk processing (as identified in row 208), an additional check is performed to evaluate the address of the invoked/called function found in a cache entry is executable as shown in block 212. During the stack walk processing, an address of an invoked function (e.g., originating caller function is identified). If an address of an invoked function is found in a cache entry, then the call is suspicious and an alert is triggered. Each entry present in the cache structure represents a part of memory that has been recently allocated with as executable (e.g., by a flag such as or similar to "EXECUTE"), and is thus a potential piece of memory that could host malicious code. If the anti-exploit technology intercepts a call to API functions such as or similar to NtCreateProcess / NtCreateProcessEx /

LdrLoadDll from one of such entries, it automatically marks this behavior as suspicious and potentially malicious.

[0043] Figure 3 illustrates an exemplary method 300 for implementation of anti-exploit systems and methods described herein. As an example, method 300 may be executed by an exemplary system such as system 100 of Figure 1. In other examples, method 300 may be executed on a device comprising at least one processor configured to store and execute operations, programs or instructions. However, method 300 is not limited to such examples. In other examples, method 300 may be performed an application or service executing the anti-exploit technology.

[0044] Method 300 begins at operation 302 where a memory space of a process is monitored for execution of at least one of a plurality of functions. Examples of functions monitored are described as part of the description of Figure 1. As an example, operation 302 monitors functions associated with memory management in the memory space by a user mode function (e.g., a call initiated from a user mode). In at least one example, operation 302 further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a function hooking technique to hook a lowest level user mode function of a called process (e.g., API). In examples, the monitoring may further comprise detecting an attempt by unidentifiable code to allocate a new executable page of memory and monitoring the allocated new executable page of memory.

[0045] Flow proceeds to operation 304 where stack walk processing is performed on a hooked and/or monitored function. When one of the plurality of functions is invoked, the stack walk processing is executed for a stack frame associated with an invoked function (e.g., originating caller function). Execution of the stack walk processing is described in further detail in the description of Figure 1 and is a process that walks a stack frame for a hooked functioned from a lowest level user mode function to an address of the invoked function/originating caller function. Operation 304 further comprises performing one or more memory checks during the stack walk processing. Examples of memory checks

that are performed are described in detail in the description of Figure 2. In one example, an originating address associated with the invoked function is identified.

[0046] Flow proceeds to decision operation 306 where a determination is made as to whether an alert of suspicious behavior is triggered based on execution of the one or more memory checks performed during the stack walk processing. For example, chart 200 of Figure 2 identifies timing associated with performance of specific memory checks. In some examples, an alert of suspicious behavior is triggered before an address of an originating caller function is reached in the stack walk processing. In other examples, each memory check is performed before an alert is triggered. If decision operation 306 determines that no alert of suspicious behavior is triggered, then flow proceeds to operation 308 where execution of code (e.g., a payload) associated with an invoked function is allowed. If decision operation 306 determines that an alert of suspicious behavior is triggered, the flow proceeds to operation 310 where execution of code associated with an invoked function is prevented. As an example, operation 310 takes action to prevent execution of a payload for the invoked function. In some example, method 300 comprises an operation of reporting suspicious behavior (operation 312). Data collected from tracking identification of potentially malicious behavior and detection of malicious behavior (as well as successful cases where execution of malicious behavior was prevented) may be useful in tracking security exploits, statistical analysis of the anti-exploit technology, and augmenting anti-exploit technology to improve over time.

[0047] Figure 4 and the additional discussion in the present specification are intended to provide a brief general description of a suitable computing environment in which the present invention and/or portions thereof may be implemented. Although not required, the embodiments described herein may be implemented as computer-executable instructions, such as by program modules, being executed by a computer, such as a client workstation or a server. Generally, program modules include routines, programs, objects, components, data structures and the like that perform particular tasks or implement particular abstract data types. Moreover, it should be appreciated that the invention and/or portions thereof may be practiced with other computer system configurations, including

Trend Micro, Inc.
EX1006-210

hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0048] Figure 4 illustrates one example of a suitable operating environment 400 in which one or more of the present embodiments may be implemented. This is only one example of a suitable operating environment and is not intended to suggest any limitation as to the scope of use or functionality. Other well-known computing systems, environments, and/or configurations that may be suitable for use include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, programmable consumer electronics such as smart phones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0049] In its most basic configuration, operating environment 400 typically includes at least one processing unit 402 and memory 404. Depending on the exact configuration and type of computing device, memory 404 (storing, among other things, anti-exploit module(s), e.g., Anti-exploit applications, APIs, programs etc. and/or other components or instructions to implement or perform the system and methods disclosed herein, etc.) may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.), or some combination of the two. This most basic configuration is illustrated in FIG. 4 by dashed line 506. Further, environment 400 may also include storage devices (removable, 408, and/or non-removable, 410) including, but not limited to, magnetic or optical disks or tape. Similarly, environment 400 may also have input device(s) 414 such as keyboard, mouse, pen, voice input, etc. and/or output device(s) 416 such as a display, speakers, printer, etc. Also included in the environment may be one or more communication connections, 412, such as LAN, WAN, point to point, etc.

Trend Micro, Inc.
EX1006-211

[0050] Operating environment 400 typically includes at least some form of computer readable media. Computer readable media can be any available media that can be accessed by processing unit 402 or other devices comprising the operating environment. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium which can be used to store the desired information. Computer storage media does not include communication media.

[0051] Communication media embodies computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[0052] The operating environment 400 may be a single computer operating in a networked environment using logical connections to one or more remote computers. The remote computer may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above as well as others not so mentioned. The logical connections may include any method supported by available communications media. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

Trend Micro, Inc.
EX1006-212

[0053] The different aspects described herein may be employed using software, hardware, or a combination of software and hardware to implement and perform the systems and methods disclosed herein. Although specific devices have been recited throughout the disclosure as performing specific functions, one of skill in the art will appreciate that these devices are provided for illustrative purposes, and other devices may be employed to perform the functionality disclosed herein without departing from the scope of the disclosure.

[0054] As stated above, a number of program modules and data files may be stored in the system memory 404. While executing on the processing unit 402, program modules 408 (e.g., applications, Input/Output (I/O) management, and other utilities) may perform processes including, but not limited to, one or more of the stages of the operational methods described herein such as method 300 illustrated in Figure 3, for example.

[0055] Furthermore, examples of the invention may be practiced in an electrical circuit comprising discrete electronic elements, packaged or integrated electronic chips containing logic gates, a circuit utilizing a microprocessor, or on a single chip containing electronic elements or microprocessors. For example, examples of the invention may be practiced via a system-on-a-chip (SOC) where each or many of the components illustrated in FIG. 4 may be integrated onto a single integrated circuit. Such an SOC device may include one or more processing units, graphics units, communications units, system virtualization units and various application functionality all of which are integrated (or "burned") onto the chip substrate as a single integrated circuit. When operating via an SOC, the functionality described herein may be operated via application-specific logic integrated with other components of the operating environment 400 on the single integrated circuit (chip). Examples of the present disclosure may also be practiced using other technologies capable of performing logical operations such as, for example, AND, OR, and NOT, including but not limited to mechanical, optical, fluidic, and quantum technologies. In addition, examples of the invention may be practiced within a general purpose computer or in any other circuits or systems.

Trend Micro, Inc.
EX1006-213

[0056] This disclosure described some aspects of the present technology with reference to the accompanying drawings, in which only some of the possible embodiments were shown. Other aspects may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these aspects were provided so that this disclosure was thorough and complete and fully conveyed the scope of the possible embodiments to those skilled in the art.

[0057] Although specific aspects were described herein, the scope of the technology is not limited to those specific embodiments. One skilled in the art will recognize other embodiments or improvements that are within the scope and spirit of the present technology. Therefore, the specific structure, acts, or media are disclosed only as illustrative embodiments. The scope of the technology is defined by the following claims and any equivalents therein.

Trend Micro, Inc.
EX1006-214

Claims

What is claimed is:

1. A computer-implemented method comprising:

monitoring a memory space of a process for execution of at least one of a plurality of functions;

executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when, during the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

2. The method according to claim 1, wherein performing the memory check occur before an address of an originating caller function is reached.

3. The method according to claim 1, further comprising:

identifying an address associated with the invoked function; and

when the address of the invoked function address is found in a cache, preventing execution of a payload for the invoked function.

Trend Micro, Inc.
EX1006-215

4. The method according to claim 1, wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function.

5. The method according to claim 1, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

6. The method according to claim 1, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

7. The method according to claim 1, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

8. The method according to claim 6, wherein performing the one or more memory checks comprises evaluating state information associated with a cache entry for the hooked function.

9. The method according to claim 8, wherein when an address of the invoked function is found in a cache, preventing execution of a payload for the invoked function.

10. A system comprising:

at least one memory; and

at least one processor connected with the memory configured to perform operation of:

monitoring a memory space of a process for execution of at least one of a plurality of functions;

Trend Micro, Inc.
EX1006-216

executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, one or more memory checks to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when, during the performing of the one or more memory checks detect at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, the method further comprising preventing execution of a payload for the invoked function.

11. The system according to claim 10, wherein the performing of the one or more memory checks occur before an address of an originating caller function is reached.

12. The system according to claim 10, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

13. The system according to claim 10, wherein the executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to an originating address of the invoked function.

14. The system according to claim 10, wherein the monitoring further comprises monitoring functions associated with memory management in the memory space by a user mode function.

15. The system according to claim 10, wherein the monitoring further comprises applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, and wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function.

16. The system according to claim 10, wherein the plurality of functions comprises an NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll function.

17. The system according to claim 15, wherein performing of the memory checks comprises evaluating state information associated with a cache entry for the hooked function.

18. The system according to claim 17, wherein when an address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function.

19. A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

monitoring a memory space of a process for execution of at least one of a plurality of functions;

executing stack walk processing upon invocation of one of the plurality of functions in the monitored memory space; and

performing, during the executing of the stack walk processing, at least one memory check to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:

code execution is attempted from non-executable memory,

a base pointer is identified as being invalid,

an invalid stack return address is identified,

attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack,

a return address is detected as being inside a virtual memory area, and

a low level user mode function is attempted to be executed in a cache, wherein the cache is evaluated for an address of the invoked function, and

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function.

20. The computer-readable storage device according to claim 19, wherein performing of the memory check to determine if code execution is attempted from non-executable memory, the base pointer is identified as being invalid, an invalid stack return address is identified, execution of a return-oriented programming technique is attempted, the base pointer is detected as being outside a current thread stack, and the return address is detected as being inside a virtual memory area, occurs before an address of the invoked function is reached, and

wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing.

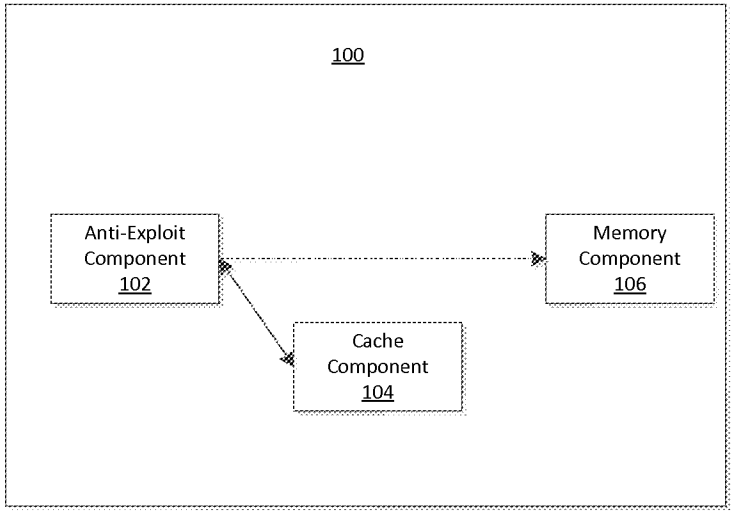
Trend Micro, Inc.
EX1006-219

Abstract

In non-limiting examples, anti-exploit systems and methods described herein monitor a memory space of a process for execution of functions. Stack walk processing is executed upon invocation of one of the functions in the monitored memory space. During execution of the stack walk processing, at least one memory check is performed to detect suspicious behavior. An alert of suspicious behavior is triggered when the performing of the memory check detects at least one of: code execution attempted from non-executable memory, identification of an invalid base pointer, identification of an invalid stack return address, attempted execution of a return-oriented programming technique, the base pointer is outside a current thread stack, and a return address is detected as being inside a virtual memory area. If an alert of suspicious behavior is triggered, execution of a payload is prevented for the invoked function.

Trend Micro, Inc.
EX1006-220

FIG. 1



Trend Micro, Inc.
EX1006-221

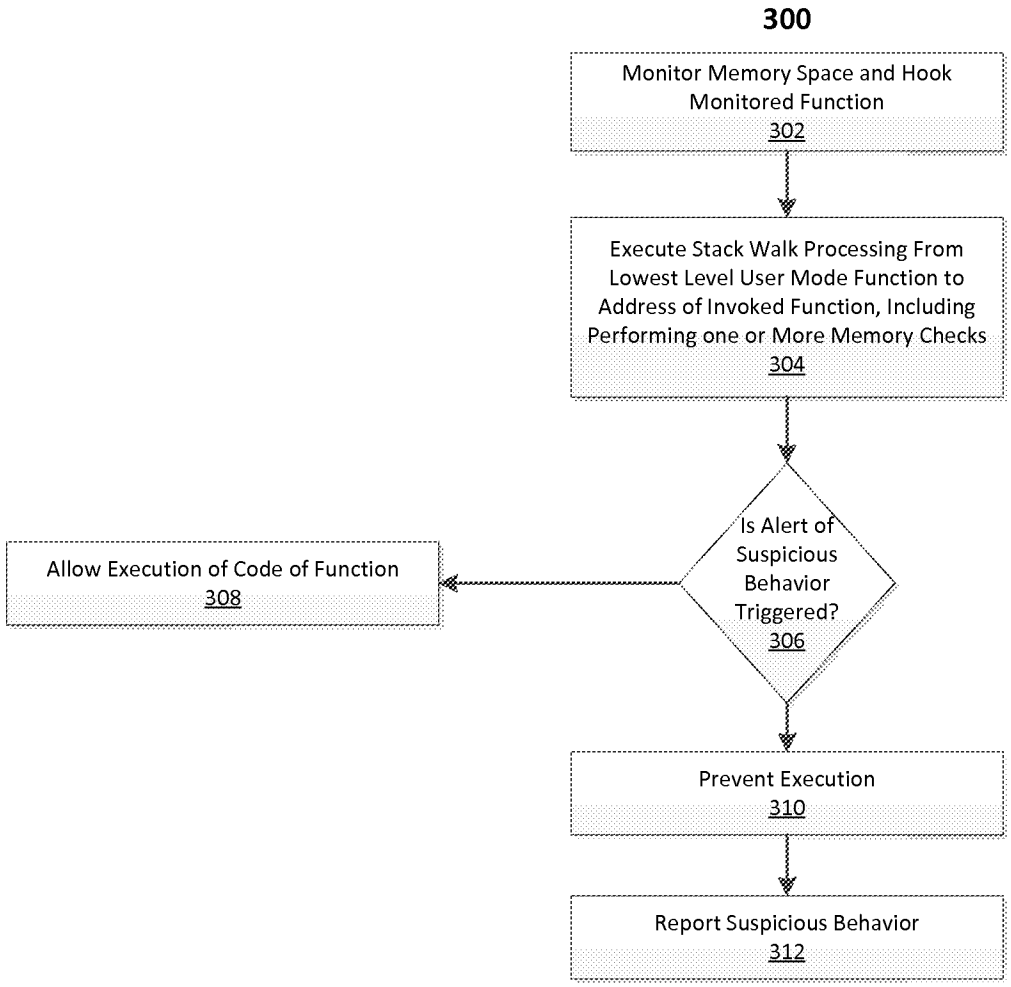
FIG. 2

200

Timing Associated with Execution of Memory Check 202	Memory Check Executed During Stack Walk Processing For Called Function 204
Before Address is Reached for Originating Caller Function 206	• Is Code Execution Attempted From Non-Executable Memory? • Is Base Pointer Identified As Being Invalid? • Is An Invalid Stack Return Address Identified? • Is Execution Of a Return-Oriented Programming Technique Attempted? • Is Base pointer Detected As Being Outside a Current Thread Stack? • Is Return Address Detected as Being Inside a Virtual Memory Area? Block 210
Once Address is Reached for Originating Caller Function 208	• Is Execution Attempted for Originating Caller Function/ Low Level User Mode Function in Cache? Block 212

Trend Micro, Inc.
EX1006-222

FIG. 3


300
Monitor Memory Space and Hook Monitored Function
302
Execute Stack Walk Processing From Lowest Level User Mode Function to Address of Invoked Function, Including Performing one or More Memory Checks
304
Is Alert of Suspicious Behavior Triggered?
306
Allow Execution of Code of Function
308
Prevent Execution
310
Report Suspicious Behavior
312

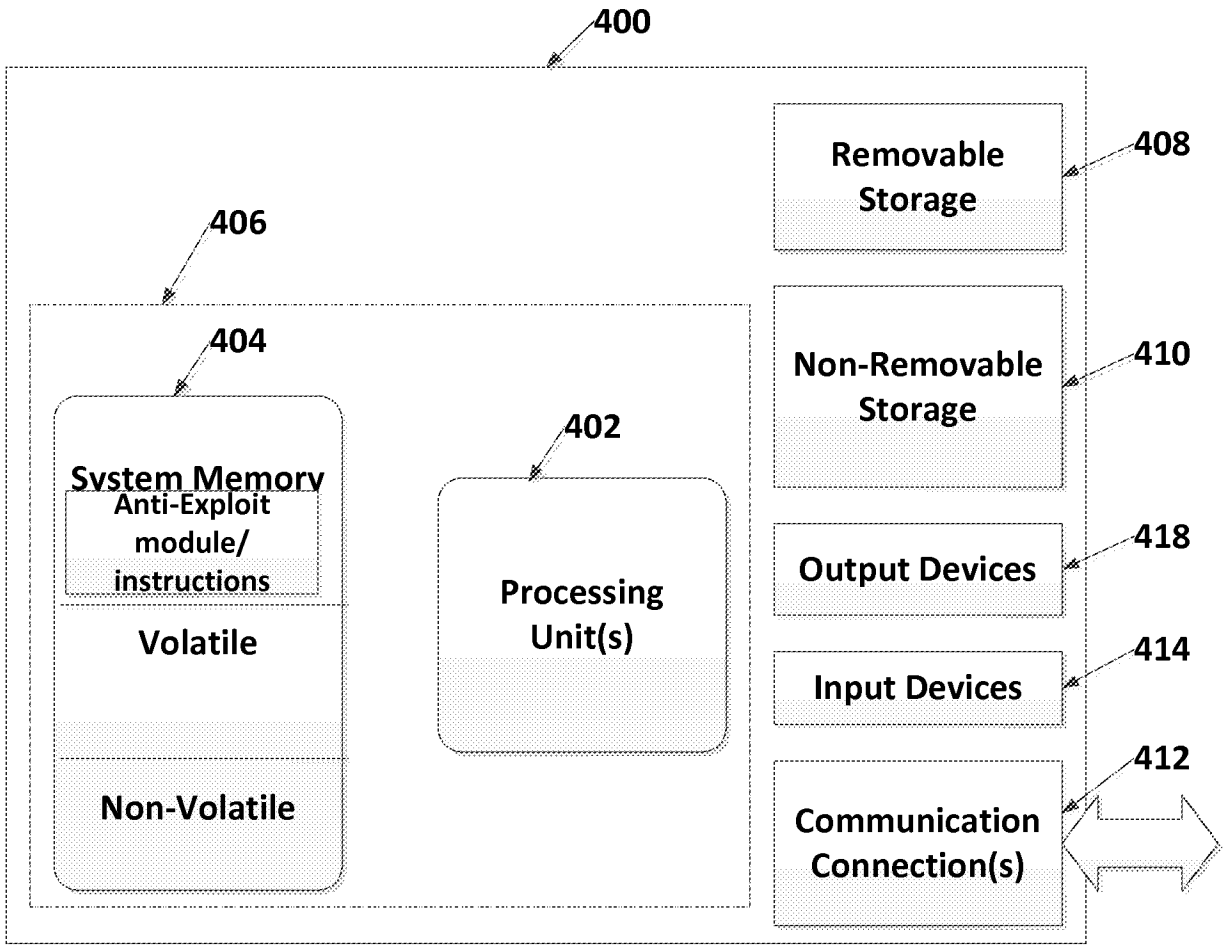


FIG. 4

Trend Micro, Inc.
EX1006-224

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Marco Giuliani Date (Optional): 23/1/2015

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Marco Bizzarri Date (Optional): 28/01/2015

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Benedetto Voltattorni Date (Optional): 27/01/15

Signature: Benedetto Voltattorni

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DETECTING AND PREVENTING EXECUTION OF SOFTWARE EXPLOITS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Johannes Mayr Date (Optional): JAN-27-2015

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.